CA Enterprise Log Manager

Guida all'implementazione

r12.1 SP3



Riferimenti ai prodotti CA

Questo documento è valido per i seguenti prodotti di CA:

- CA Access Control
- CA Audit
- CA ACF2™
- CA Directory
- CA Embedded Entitlements Manager (CA EEM)
- CA Enterprise Log Manager
- CA Identity Manager
- CA IT Process Automation Manager (CA IT PAM)
- CA NSM
- CA Security Command Center (CA SCC)
- CA Service Desk
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

Contattare il servizio di Supporto tecnico

Per l'assistenza tecnica in linea e un elenco completo delle sedi, degli orari del servizio di assistenza e dei numeri di telefono, contattare il Supporto tecnico visitando il sito Web all'indirizzo http://www.ca.com/worldwide.

Modifiche apportate alla documentazione

Di seguito sono riportati gli aggiornamenti apportati alla documentazione dall'ultimo rilascio.

- Considerazioni sugli utenti CA Audit - Questo capitolo esistente è stato aggiornato per includere una nota alla configurazione del plug-in evento iTechnology.
- Virtualizzazione - Questo capitolo esistente è stato aggiornato per includere la modifica dei parametri necessari per la distribuzione del modello OVF.

Ulteriori informazioni:

Funzionamento della sottoscrizione senza proxy in linea (a pagina 60)
Agenti e certificati degli agenti (a pagina 67)
Aggiornamento di un server CA EEM remoto (a pagina 95)
Disabilitare l'accesso ODBC e JDBC al deposito eventi di log (a pagina 95)
Abilitare operazioni di modalità FIPS (a pagina 96)
Visualizzare il dashboard di agente (a pagina 97)
Considerazioni sull'installazione di sistemi con unità di SAN (a pagina 101)
Installazione con unità SAN disabilitate (a pagina 102)
Disattivazione delle unità SAN (a pagina 103)
Impostazione di una configurazione con più percorsi per l'archiviazione SAN (a pagina 103)
Creazione di un volume logico (a pagina 105)
Preparazione di un volume logico per CA Enterprise Log Manager (a pagina 106)
Riavvio del server CA Enterprise Log Manager (a pagina 107)
Installazione con unità SAN abilitate (a pagina 108)
Assegnazioni delle porte predefinite (a pagina 112)
Spostamento del database e diagramma di flusso delle strategie di backup (a pagina 161)
Configurazione dell'autenticazione non interattiva per archiviazione automatica (a pagina 162)
Esempio: Configurazione dell'autenticazione non interattiva per hub e spoke (a pagina 163)
Configurazione delle chiavi per la prima coppia raccolta/rapporto (a pagina 164)
Configurazione delle chiavi per una coppia aggiuntiva raccolta/rapporto (a pagina 165)
Creazione di un file della chiave pubblica sul server di rapporto e impostazione della proprietà del file (a pagina 166)
Convalida dell'autenticazione non interattiva tra i server di raccolta e i server di rapporto (a pagina 168)
Creazione di una struttura di directory con proprietà sul server di archiviazione remoto (a pagina 168)
Configurazione delle chiavi per la coppia di archiviazione rapporto/remoto (a pagina 169)
Impostazione della proprietà del file della chiave sul server di archiviazione remoto (a pagina 170)
Convalida dell'autenticazione non interattiva tra i server di rapporto e i server di archiviazione (a pagina 171)
Esempio: Configurazione dell'autenticazione non interattiva tra tre server (a pagina 172)
Esempio: archiviazione automatica fra tre server (a pagina 173)
Considerazioni su ODBC Server (a pagina 181)
Diagramma di flusso della distribuzione delle sottoscrizioni (a pagina 185)

Sommario

Capitolo 8: Lavorare con la libreria di perfezionamento eventi 229

Appendice A: Considerazioni per gli utenti CA Audit 233

Appendice B: Considerazioni per gli utenti CA Access Control 259

Appendice E: CA Enterprise Log Manager e virtualizzazione 303

Glossario 385

Indice 417

Capitolo 1: Introduzione

Questa sezione contiene i seguenti argomenti:

Informazioni sulla guida

Questa *Guida di implementazione di CA Enterprise Log Manager* contiene le istruzioni necessarie per pianificare, installare e configurare CA Enterprise Log Manager in modo da ricevere registri evento da origini evento della propria rete. La guida è organizzata in modo che ogni attività inizi con una descrizione del processo e dei relativi obiettivi. Di solito i processi vengono seguiti da argomenti importanti e quindi da una o più procedure utili per completare l'obiettivo.

La *Guida di implementazione di CA Enterprise Log Manager* è indirizzata agli amministratori di sistema che hanno la responsabilità di installare, configurare e gestire la manutenzione di una soluzione di raccolta di registro, di creare utenti e di assegnare o definire i relativi ruoli e accessi, oltre che di occuparsi della manutenzione dei dati di backup.

Questa guida è utile anche al personale a cui occorrono informazioni sulle procedure necessarie per eseguire le seguenti operazioni:

- Configurare un connettore o un adattatore per raccogliere dati di evento
- Configurare servizi per controllare i rapporti, la conservazione dei dati, il backup e l'archiviazione
- Configurare una federazione di server CA Enterprise Log Manager
- Configurare una sottoscrizione per ottenere aggiornamenti di contenuto, configurazione e del sistema operativo

Ecco un riassunto dei contenuti:

Sezione	**Descrizione**
Pianificazione dell'ambiente	Descrive le attività di pianificazione per aree come la raccolta dei registri, gli agenti, la federazione, la gestione degli utenti e degli accessi, aggiornamenti della sottoscrizione e ripristino di emergenza.

Sezione	Descrizione
Installazione di CA Enterprise Log Manager	Fornisce fogli di calcolo per la raccolta delle informazioni necessarie e istruzioni dettagliate sull'installazione di CA Enterprise Log Manager e sulla verifica dell'installazione corretta.
Configurazione di utenti e accessi di base	Fornisce istruzioni per individuare un archivio utente e creare l'utente amministrativo iniziale per la configurazione dell'altro utente e dei dettagli di accesso.
Configurazione dei servizi	Fornisce istruzioni per la configurazione di servizi fra cui i filtri globali e locali, l'archivio registro eventi, il server di rapporto e le opzioni di sottoscrizione.
Configurazione della raccolta eventi	Fornisce argomenti e istruzioni necessari per utilizzare o configurare i componenti della libreria di perfezionamento eventi, fra cui i file di analisi e di mapping e gli adattatori di CA.
Creazione di federazioni	Descrive tipi diversi di federazioni e fornisce istruzioni per la creazione di relazioni federate tra server CA Enterprise Log Manager e per la visualizzazione di un grafico di federazione.
Lavorare con la libreria di perfezionamento eventi	Fornisce informazioni di alto livello sul lavoro con i file di analisi dei messaggi e di mapping dei dati.
Considerazioni per gli utenti di CA Audit	Descrive le interazioni che è possibile implementare fra CA Enterprise Log Manager e CA Audit, i metodi per configurare gli iRecorder e i criteri e quelli per importare dati dal proprio database di CA Audit Collector.
Considerazioni per gli utenti di CA Access Control	Descrive come eseguire l'integrazione con CA Access Control, come modificare i criteri di CA Audit per inviare eventi a CA Enterprise Log Manager, come configurare un iRecorder CA Access Control per inviare eventi a CA Enterprise Log Manager e come importare eventi di CA Access Control da un database CA Audit Collector,
Considerazioni su CA IT PAM	Descrive il processo di installazione di CA IT PAM tale per cui il componente EEM su CA Enterprise Log Manager di gestione gestisca l'autenticazione.
Ripristino di emergenza	Descrive le procedure di backup, di ripristino e di sostituzione in grado di garantire il ripristino della propria soluzione di gestione registri in caso di gravi avarie.
CA Enterprise Log Manager e virtualizzazione	Descrive la procedura per la creazione e la configurazione di una macchina virtuale in grado di contenere un server CA Enterprise Log Manager.

Nota: per informazioni sul supporto del sistema operativo o sui requisiti di sistema, consultare le *Note della versione*. Per una panoramica di base di CA Enterprise Log Manager e uno scenario di utilizzo, consultare la *Guida di panoramica*. Per informazioni sull'utilizzo e sulla manutenzione del prodotto, consultare la *Guida all'amministrazione* .Per assistenza sull'utilizzo di una pagina di CA Enterprise Log Manager, consultare la Guida in linea.

Capitolo 2: Pianificazione dell'ambiente

Questa sezione contiene i seguenti argomenti:

Pianificazione server

Il primo passaggio della pianificazione dell'ambiente consiste nel determinare quanti server CA Enterprise Log Manager sono necessari e quale ruolo verrà svolto da ogni server. I ruoli includono:

- Gestione

  Archivia contenuti e configurazioni definiti dall'utente. Autentica anche gli utenti e autorizza l'accesso alle funzioni.

- Raccolta

  Riceve registri eventi dal suo agente; esegue il trattamento degli eventi.

- Rapporti

  Elabora le query dei degli eventi raccolti, sia query che rapporti su richiesta e anche avvisi e rapporti pianificati.

- Punto di ripristino

  Riceve i database dei registri eventi ripristinati per l'analisi degli eventi passati

Il primo server che si installa è il server di gestione; questo server può eseguire anche altri ruoli. È possibile disporre solo di un server di gestione in un'unica rete CA Enterprise Log Manager. Ogni rete CA Enterprise Log Manager deve disporre di un server di gestione.

Le architetture possibili includono:

- Sistema a server unico, dove il server svolge tutti gli altri ruoli
- Sistema a due server, in cui il server di gestione svolge tutti i ruoli tranne la raccolta. La raccolta viene eseguita da un server dedicato a questo ruolo.
- Sistema a più server, in cui ogni server è dedicato a un unico ruolo.

I dettagli sui ruoli del server e delle architetture vengono descritti di seguito.

Ruoli dei server

Un sistema CA Enterprise Log Manager può disporre di uno o più server. Dedicando server diversi a ruoli diversi si ottimizzano le prestazioni. Ma è possibile utilizzare qualsiasi server per eseguire ruoli diversi o tutti i ruoli, a propria discrezione. Considerare il carico di elaborazione associato ad ogni ruolo di server rispetto ad altri fattori rilevanti nell'ambiente quando si stabilisce come dedicare ogni server che viene installato.

- Server di amministrazione

  Il ruolo di server di gestione è, per impostazione predefinita, svolto dal primo server CA Enterprise Log Manager che si installa. Il server di gestione esegue queste funzioni principali:

  - Opera come repository comune per tutti i server che si registrano con questo server. Nello specifico, archivia gli utenti delle applicazioni, i gruppi di applicazioni (ruoli), i criteri, i calendari e gli AppObjects.
  - Se si configura l'archivio utente come archivio interno, archivia gli utenti globali, i gruppi globali e i criteri delle password. Se l'archivio utente configurato è un riferimento a un archivio utente esterno, carica i dettagli dell'account dell'utente globale e i dettagli del gruppo globale dall'archivio utente di riferimento.
  - Gestisce le autorizzazioni degli utenti con un file ad alta velocità mappato nella memoria. Autentica gli utenti all'accesso in base alla configurazione di utenti e gruppi. Autorizza gli utenti ad accedere a varie parti dell'interfaccia utente in base a criteri e calendari.
  - Riceve tutti gli aggiornamenti di contenuti e configurazioni scaricati attraverso la sottoscrizione.

  Può essere presente solo un server di gestione attivo in una rete CA Enterprise Log Manager di server, ma è possibile disporre di un server di gestione failover (inattivo). Se si crea più di una rete CA Enterprise Log Manager, ognuna deve disporre del proprio server di gestione attivo.

- Server di raccolta

  In un sistema a server unico, il server di gestione svolge il ruolo di server di raccolta. In un sistema di due o più server, considerare l'utilizzo di un server di raccolta dedicato. Un server di raccolta svolge queste funzioni:

  - Supporta la configurazione di connettori.
  - Accetta i log di eventi in entrata da connettori sugli agenti.
  - Perfeziona i log di eventi in entrata, attività che prevede l'analisi di tutti i messaggi ed il mapping dei dati in formato CEG che consente una presentazione uniforme dei dati degli eventi da diverse origini di eventi.
  - inserisce i log di eventi nel database hot e comprime il database hot quando questo raggiunge le dimensioni configurate in un database warm.
  - Archivia automaticamente il database warm al relativo server di rapporto in base alla pianificazione configurata.

    Importante: Quando si utilizzano server separati per la raccolta e i rapporti, è necessario configurare l'autenticazione non interattiva e l'archiviazione automatica una volta all'ora dal server di raccolta al server di rapporto.

  Considerare il volume di eventi generato dalle fonti degli eventi quando si stabilisce se dedicare i server alla raccolta e al trattamento degli eventi. Valutare inoltre quanti server di raccolta eseguono l'archiviazione automatica dei dati in un singolo server di rapporto.

- Server di rapporto

  In un sistema a server unico o doppio, il server di gestione svolge il ruolo di server di rapporto. In un sistema con diversi server, considerare di dedicare uno o più server ai rapporti. Un server di rapporto svolge queste funzioni:

  - Riceve nuovi database di eventi perfezionati dai server di raccolta, in quanto sono state configurate l'autenticazione non interattiva e l'archiviazione automatica.
  - Elabora prompt, query e rapporti a richiesta.
  - Elabora avvisi e rapporti pianificati.
  - Supporta procedure guidate per la creazione di query e rapporti personalizzati.
  - Sposta i vecchi database in un server di archiviazione remoto quando l'autenticazione non interattiva e l'archiviazione automatica.sono state configurate da un server di rapporto in un server di archiviazione remoto.

  Se si ha intenzione di generare diversi rapporti e avvisi complessi su un server con elevata attività a richiesta, considerare di dedicare un server ai rapporti.

- Server di archiviazione remoto

  Un server di archiviazione remoto, che non è un server CA Enterprise Log Manager, svolge questa funzione:

  - Riceve database compressi e archiviati automaticamente dai server di rapporto a intervalli configurati prima che tali database possano essere eliminati poiché obsoleti o per mancanza di spazio su disco. L'archiviazione automatica evita all'utente di spostare manualmente i database.
  - Archivia localmente i database cold. Inoltre, è possibile copiare o spostare questi database in una posizione decentralizzata per l'archiviazione a lungo termine. I database cold tipicamente vengono conservati per il numero di anni stabilito dalle agenzie di governative.

  I server di archiviazione remoti non fanno mai parte di una federazione CA Enterprise Log Manager. Tuttavia, essi meritano considerazione durante la pianificazione dell'architettura.

- Server punto di ripristino

  I server di rapporto agiscono di solito come server di punto di ripristino per i database di cui disponevano. Se la rete è ampia, considerare di dedicare un server CA Enterprise Log Manager a questo ruolo. Un server punto di ripristino svolge queste funzioni:

  - Viene utilizzato per investigare i registri dei vecchi eventi.
  - Riceve database ripristinati da un server di archiviazione remoto che conserva tutti i database cold. È possibile utilizzare l'utilità restore-ca-elm.sh per spostare i database al punto di ripristino se è stata configurata l'autenticazione non interattiva dal server di archiviazione al punto di ripristino.
  - Esegue la ricatalogazione del catalogo degli archivi per aggiungere i database ripristinati alle registrazioni.
  - Conserva registrazioni per lunghezze temporali configurate diverse, a seconda del metodo di ripristino.

  Il vantaggio di disporre di un punto di ripristino dedicato è che è possibile escludere questo server dalla federazione per garantire che nessun rapporto federato contenga vecchi dati ripristinati. Tutti i rapporti generati sul server punto di ripristino riflettono solo i dati degli eventi dai database ripristinati.

Dedicare un server ad alcuni ruoli non significa che non è possibile svolgere funzioni associate ad altri ruoli. Si consideri un ambiente con server di raccolta dedicati e un server di rapporto. Se si vuole pianificare un avviso per controllare una condizione di un server di raccolta, perché è importante in termini di tempo ricevere una notifica il prima possibile, si dispone di questa flessibilità.

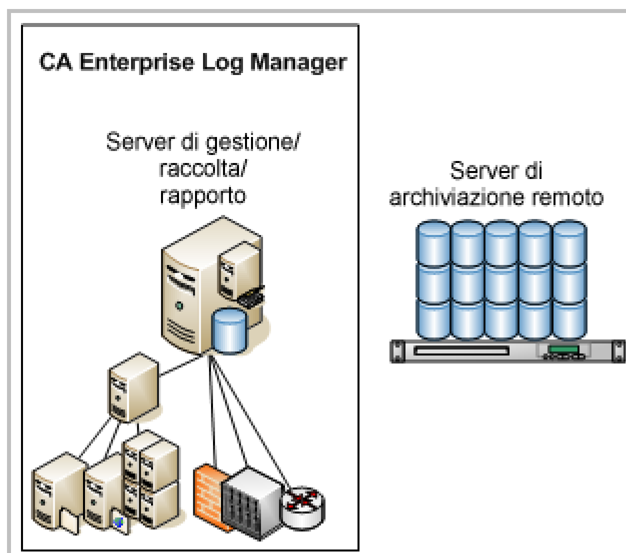
Esempio: Architetture di rete

L'architettura più semplice CA Enterprise Log Manager è un sistema a server singolo, in cui un server CA Enterprise Log Manager svolge tutti i ruoli:

- Il server CA Enterprise Log Manager di gestione, raccolta e rapporto gestisce la configurazione e i contenuti, la raccolta e il perfezionamento di eventi, le query e i rapporti.

  Nota: un server remoto diverso da -CA Enterprise Log Manager archivia i database dei registri eventi archiviati .

Questa configurazione è adatta per l'elaborazione di un basso volume di eventi e pochi rapporti pianificati, come nel sistema di prova.

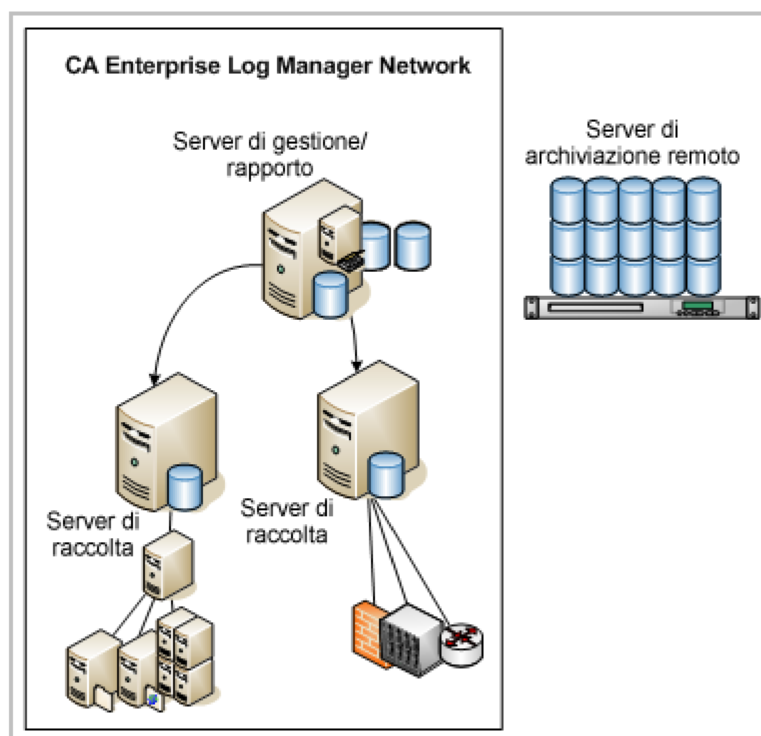


La successiva architettura più semplice è un sistema a più server in cui il primo CA Enterprise Log Manager installato svolge la maggior parte dei ruoli:

- Il server CA Enterprise Log Manager di gestione e dei rapporti gestisce la configurazione/i contenuti e le query e i rapporti.
- I CA Enterprise Log Manager di raccolta gestiscono la raccolta e il trattamenti di eventi.

Nota: un server remoto diverso da -CA Enterprise Log Manager è impostato per archiviare i database dei registri di eventi archiviati.

Questa architettura è adatta a una rete con volume di eventi ridotto. Le frecce indicano che la funzionalità di gestione del server di gestione/rapporto mantiene le impostazioni globali valide per tutti i server Se vi sono più server di raccolta, questa architettura viene definita "hub e spoke."

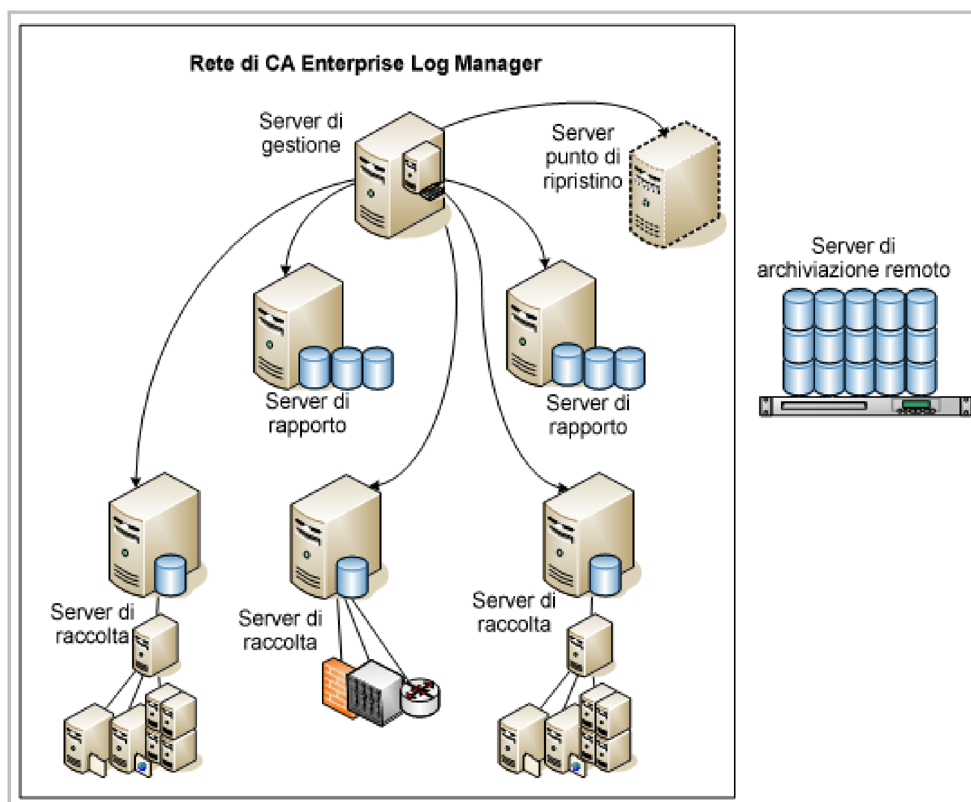


In una rete ampia con volume di eventi elevato, molti rapporti e avvisi pianificati complessi e personalizzazione costante, è possibile dedicare uno o più server CA Enterprise Log Manager a ruoli singoli:

- Il server CA Enterprise Log Manager di gestione si occupa della gestione della configurazione/dei contenuti.
- Il CA Enterprise Log Manager dei rapporti gestisce query e rapporti.
- I CA Enterprise Log Manager di raccolta gestiscono la raccolta e il trattamenti di eventi.
- Inoltre, un punto di ripristino CA Enterprise Log Manager gestisce l'analisi di eventi da database di archivi ripristinati.

Nota: un server remoto diverso da -CA Enterprise Log Manager è impostato per archiviare i database dei registri di eventi archiviati.

Questa configurazione è ideale per reti molto vaste. Le frecce indicano che il server di gestione mantiene le impostazioni globali valide per tutti i server



Pianificazione della raccolta registri

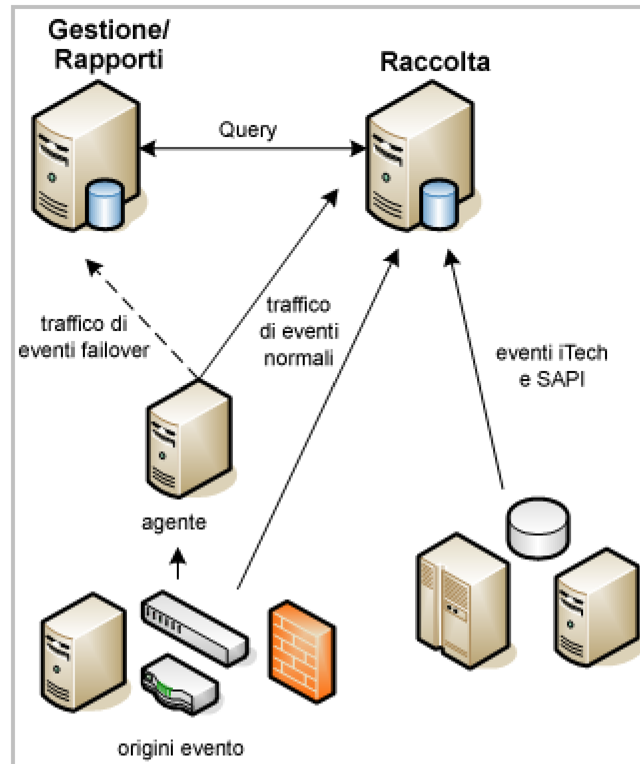
La pianificazione della raccolta dei registri per la rete si basa sul numero di eventi al secondo (eps) da elaborare per l'archiviazione e sulla durata del tempo di memorizzazione dei dati online (in questo senso, *online* significa in uno stato che è possibile trovare immediatamente). Di solito, è possibile memorizzare i dati online per 30-90 giorni.

Ogni rete dispone del proprio volume di eventi come funzione del numero di periferiche, tipi di periferiche e livello di adattamento delle periferiche e delle applicazioni di rete, come i firewall, alle richieste di informazioni sugli eventi aziendali. Ad esempio, alcuni firewall possono generare enormi volumi di eventi non necessari in base a come vengono configurati.

Si consiglia di pianificare la raccolta degli eventi in modo che il volume totale di eventi sia distribuito sui server CA Enterprise Log Manager senza forzare nessuno di essi a superare il carico di lavoro costante normale. Per mantenere prestazioni di picco con volumi di eventi a livello aziendale, si consiglia di installare almeno due server CA Enterprise Log Manager federati:

- Un server di rapporto CA Enterprise Log Manager che si occupa di query e rapporti, gestione di avvisi, aggiornamenti delle sottoscrizioni e autenticazione e autorizzazione degli utenti.
- Uno o più server di raccolta CA Enterprise Log Manager configurati specificamente per massimizzare gli inserimenti nel database.

La seguente illustrazione rappresenta un semplice esempio di questo tipo di rete CA Enterprise Log Manager federata. Due server CA Enterprise Log Manager, uno dedicato ai rapporti e l'altro alla raccolta, gestiscono il traffico degli eventi da una serie di origini. Entrambi i server possono condividere dati tra di loro per le query, i rapporti e gli avvisi.



Il server di *raccolta* gestisce innanzitutto il traffico dei registri eventi in ingresso e si focalizza sugli inserimenti nei database. Utilizza criteri di memorizzazione a breve termine dei dati, per 24 ore o meno. Uno script automatizzato sposta i registri eventi archiviati in un server di rapporti quotidianamente o più spesso a seconda del volume di eventi. La federazione e l'utilizzo di query federate tra i due server garantisce la ricezione di rapporti precisi dai registri eventi su *entrambi* i server.

Il server di *rapporto* svolge diverse funzioni:

- Elabora le query e i rapporti.
- Pianifica e gestisce gli avvisi.
- Sposta i file archiviati in un server di archiviazione remoto.
- Fornisce la raccolta di failover di eventi raccolti dal connettore per il server di raccolta.

Uno script di backup automatizzato sposta i dati dal server di rapporto a un server remoto (archivio cold). Se si decide di ripristinare i dati dall'archivio cold, generalmente si esegue questa operazione sul server di rapporto. Se lo spazio sul server di rapporto è limitato, è possibile anche ripristinare il server di raccolta. Poiché il server di raccolta non archivia grandi quantità di dati ed è federato, i risultati del rapporto sono gli stessi.

Inoltre, il server di rapporto può funzionare come ricevitore di failover per gli eventi raccolti da un connettore su un agente remoto, se il server di raccolta smette di ricevere eventi per qualche motivo. È possibile configurare failover a livello di agente. L'elaborazione dei failover invia eventi a uno o più server CA Enterprise Log Manager alternati. La raccolta di eventi di failover non è disponibile per fonti di eventi preesistenti come raccolte dai listener SAPI e iTech.

Ulteriori informazioni:

CA Enterprise Log Manager e virtualizzazione (a pagina 303)

Pianificazione dello spazio su disco

Quando si pianifica l'ambiente, assicurarsi di disporre di spazio a sufficienza per supportare grandi volumi di eventi. Nel caso dei server di raccolta, ciò significa disporre di sufficiente spazio su disco affinché ogni server di raccolta sia in grado di contenere la propria parte di picchi di carico e i volumi di eventi standard. Per un server di rapporto, lo spazio su disco viene calcolato in base al volume degli eventi e al necessario periodo di conservazione in linea.

I database hot non vengono compressi. I database warm vengono compressi. Sia i database hot che warm sono considerati online. È possibile effettuare ricerche o creare rapporti sui loro dati. Generalmente si dispone di una quantità massima di dati pari a un periodo compreso tra 30 e 90 giorni pronti per i rapporti e la ricerca immediata in qualunque momento. Le registrazioni più vecchie di questo periodo vengono conservate in un server remoto. È possibile ripristinarle per la ricerca e i rapporti, a seconda delle esigenze.

I server di raccolta supportano database sia hot che warm. Poiché il periodo di conservazione per un server di raccolta è molto breve, da una a 23 ore, non è possibile l'archiviazione a lungo termine.

Il server di amministrazione contiene un database hot per l'inserimento dei messaggi degli eventi di automonitoraggio.

I server di rapporti supportano database hot di dimensioni inferiori e un gran numero di database warm. I server di rapporto devono inoltre disporre di spazio supplementare per supportare i file ripristinati per un determinato tempo. Quando si utilizzano periferiche collegate direttamente, le partizioni vengono estese automaticamente per consentire una maggiore capacità di archiviazione.

Informazioni sul server CA EEM

CA Enterprise Log Manager utilizza il server CA Embedded Entitlements Manager (CA EEM) internamente per gestire le configurazioni, autorizzare e autenticare gli utenti, coordinare gli aggiornamenti delle sottoscrizioni di contenuti e file binari ed eseguire altre funzioni di gestione. Nell'ambiente CA Enterprise Log Manager di base, si installa CA EEM quando si installa il server CA Enterprise Log Manager di gestione. Da questo punto CA EEM gestisce le configurazioni di tutti i server CA Enterprise Log Manager di raccolta e dei loro agenti e connettori.

È inoltre possibile scegliere di installare il server CA EEM su un server remoto utilizzando i pacchetti di installazione forniti sul disco di installazione dell'applicazione oppure è possibile utilizzare un server CA EEM esistente se si dispone di uno utilizzato con altri prodotti CA.

Il server CA EEM offre la propria interfaccia web. Tuttavia, quasi tutte le attività di configurazione e manutenzione avvengono all'interno dell'interfaccia utente CA Enterprise Log Manager. Normalmente non è necessario interagire con le funzioni server CA EEM, eccetto per configurazioni failover e per le funzioni di backup e ripristino che fanno parte del ripristino di emergenza.

Nota: l'installazione del server CA Enterprise Log Manager richiede l'utilizzo della password per l'account di amministrazione predefinito CA EEM, EiamAdmin, per una registrazione corretta di un server CA Enterprise Log Manager. Quando si installa il primo server CA Enterprise Log Manager di gestione, si crea questa nuova password come parte dell'installazione. Quando si installano server CA Enterprise Log Manager successivi utilizzando lo stesso nome di istanza dell'applicazione, si crea automaticamente un ambiente di rete in cui successivamente è possibile configurare relazioni di federazione tra i server CA Enterprise Log Manager.

Linee guida per la raccolta dei registri

Considerare le seguenti linee guida di raccolta dei registri durante la fase di pianificazione:

- Il traffico dall'agente al server CA Enterprise Log Manager è sempre crittografato, sia che utilizzi la raccolta dei registri senza agente che basata su un agente.
- Considerare l'utilizzo di un meccanismo di raccolta locale syslog come soluzione per i potenziali problemi con una consegna garantita.

Quando si stabilisce se utilizzare la raccolta diretta attraverso l'agente predefinito, la raccolta basata su agente dove questo è installato sull'host con la fonte degli eventi o la raccolta senza agente in cui questo è installato su un punto di raccolta distante dalle fonti degli eventi, considerare questi fattori:

- Piattaforme supportate

  Ad esempio, WMI funziona solo su Windows per il sensore di registro.
- Supporto di driver per alcuni sensori di registro

  Ad esempio, è necessario un driver ODBC affinché ODBC funzioni.
- Possibilità di eseguire l'accesso alla fonte degli eventi da remoto

  Ad esempio, per i registri basati su file, è necessaria un'unità condivisa affinché essi funzionino da remoto.

Pianificazione di una federazione

Per CA Enterprise Log Manager, una *federazione* è una rete di server che conserva, invia rapporti e archivia dati sugli eventi. Una federazione permette di controllare come i dati sono raggruppati ed esaminati in una rete. È possibile configurare come i server si relazionano l'uno con l'altro e quindi come le query vengono inviate da un server all'altro. Inoltre, è possibile attivare e disattivare le query federate per query specifiche, a seconda della necessità.

La decisione di utilizzare una federazione è basata sulla combinazione di volumi di eventi necessari ed esigenze aziendali di separazione e rapporti sui dati dei registri. CA Enterprise Log Manager supporta federazioni gerarchiche e a coppie e configurazioni che fondono i due tipi. Tutti i server CA Enterprise Log Manager che si vuole federare devono utilizzare lo stesso nome di istanza dell'applicazione in CA EEM. Ogni installazione di server CA Enterprise Log Manager si registra automaticamente con il CA EEM utilizzando un nome di istanza dell'applicazione.

È possibile configurare una federazione in qualsiasi momento dopo avere installato il primo server CA Enterprise Log Manager e almeno un server aggiuntivo. Tuttavia, i migliori risultati si ottengono dalla pianificazione della federazione *prima* dell'installazione. La creazione di una mappa dettagliata della federazione aiuta a completare rapidamente e con precisione le attività di configurazione.

A livello della *rete*, disporre di diversi server CA Enterprise Log Manager permette di gestire volumi maggiori di eventi. Da una prospettiva del *rapporto*, l'utilizzo di una federazione permette di controllare chi può accedere ai dati degli eventi e quanti di questi dati è possibile visualizzare.

In un ambiente di base costituito da due server, il server di gestione assume il ruolo di server di rapporto. Il server CA EEM interno sul server di gestione CA Enterprise Log Manager gestisce le configurazioni della federazione centralmente e globalmente (è possibile modificare le opzioni di configurazione da qualsiasi server CA Enterprise Log Manager all'interno della rete). Si configura il server di raccolta CA Enterprise Log Manager come figlio del server di rapporto, in modo che query e rapporti includano i dati più recenti.

Nota: se si dispone di un server CA EEM esistente che si intende utilizzare con CA Enterprise Log Manager, configurare i server CA Enterprise Log Manager nello stesso modo. Il server CA EEM remoto dedicato archivia queste configurazioni.

È inoltre possibile impostare le opzioni di configurazione locali affinché ignorino le configurazioni globali, permettendo ai server CA Enterprise Log Manager selezionati di operare in modo diverso dagli altri. Gli esempi includono l'invio di rapporti e-mail e avvisi attraverso un server di posta diverso, o la pianificazione di rapporti specifici per una sezione della rete in momenti diversi.

Ulteriori informazioni:

Federazioni gerarchiche (a pagina 222)
Federazioni a coppie (a pagina 224)
Query e rapporti in un ambiente federato (a pagina 221)
Configurazione di una federazione CA Enterprise Log Manager (a pagina 225)

Creazione di una mappa della federazione

La creazione di una mappa della federazione è un passaggio utile per la pianificazione e l'implementazione della configurazione della federazione. Più la rete è larga, più questa mappa sarà utile durante le attività della configurazione attuale. È possibile utilizzare qualsiasi grafico commerciale o programma di disegno o abbozzare la mappa a mano. Maggiori sono i dettagli forniti nella mappa, più sarà veloce la configurazione.

Creazione di una mappa della federazione

1. Avviare la mappa con due server CA Enterprise Log Manager di base, di gestione e di raccolta, e fornire i dettagli di ognuno.
2. Decidere se sono necessari altri server di raccolta e se rappresentano il livello più alto di una gerarchia o unità della combinazione.
3. Decidere quale tipo di federazione si adatta meglio alle proprie esigenze, gerarchico o a coppie.
4. Identificare le opportunità di gerarchie, rami o interconnessioni in base alle esigenze aziendali relative a rapporti, conformità e produzione di eventi.

   Ad esempio, se l'azienda dispone di uffici in tre continenti, è possibile decidere di creare tre generazioni gerarchiche. È inoltre possibile decidere di disporre a coppie le gerarchie ad un livello elevato, in modo che dirigenti senior e gestione della sicurezza possano produrre rapporti che coprono l'intera rete. È necessario come minimo federare i server CA Enterprise Log Manager di inserimento e query dell'ambiente di base.
5. Decidere quanti server CA Enterprise Log Manager in totale è necessario distribuire.

   Questo valore si basa sul numero di periferiche nella rete e sul volume di eventi che generano.
6. Decidere quanti layer di server federati sono necessari.

   Questo numero si basa in parte sulle decisioni che vengono prese nei passaggi 2 e 3.
7. Identificare i tipi di evento che ogni server CA Enterprise Log Manager riceve nella federazione.

   Se la rete ha un gran numero di periferiche basate su syslog e solo pochi server Windows, è possibile decidere di allocare un server CA Enterprise Log Manager appositamente per la raccolta eventi di Windows. Sono necessari server diversi per gestire il traffico degli eventi syslog. La pianificazione in anticipo di quali server CA Enterprise Log Manager ricevono quale tipo di eventi semplifica la configurazione dei listener e dei servizi locali.

8. Abbozzare una mappa di questa rete da utilizzare durante la configurazione dei server (figlio) CA Enterprise Log Manager federati.

   Includere i nomi e gli indirizzi IP dei DNS nella mappa, se noti. Si utilizzeranno i nomi DNS dei server CA Enterprise Log Manager per configurare le relazioni della federazione tra di essi.

Esempio: mappa federazione di una grande impresa

Quando si crea la mappa di una federazione, considerare i tipi di rapporti per cui si vogliono set diversi di dati consolidati. Ad esempio, considerare lo scenario in cui si vogliono dati consolidati utilizzando tre tipi di raggruppamenti di server:

- Tutti i server

  Per i rapporti di sistema sugli eventi di automonitoraggio, l'inclusione di tutti i server permette di valutare la salute dell'intera rete di server CA Enterprise Log Manager in una volta sola.

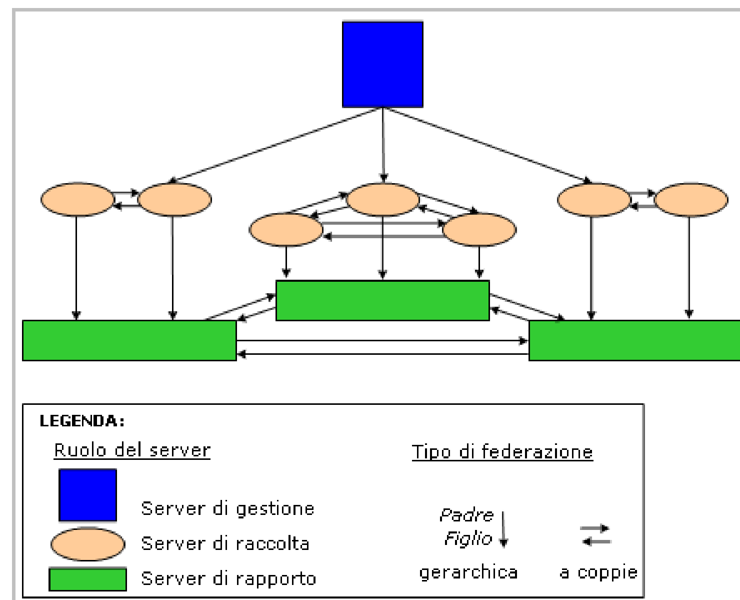
- Tutti i server di rapporto

  Per i rapporti di riepilogo e delle tendenze in cui si desidera esaminare i dati raccolti da tutti gli agenti che inviano dati a tutti i server di raccolta evitando che i server di raccolta elaborino le query sui nuovi eventi hot, è necessario eseguire rapporti federati che comprendono solo i server di rapporto.

- Un set di server di raccolta con il relativo server di rapporto

  Per i rapporti in cui si desidera che i dati siano limitati in locale con un server di rapporto, ma in cui il rapporto deve comprendere gli eventi non ancora inviati a tale server dai relativi server di raccolta, è necessario eseguire rapporti federati su questo sottoinsieme di server.

A seguire, un esempio di mappa di federazione che permette di soddisfare questi obiettivi dei rapporti:



Per implementare la realizzazione di questa mappa di federazione, è necessario intraprendere le seguenti azioni:

- Creare una federazione gerarchica dal server di gestione a un server di raccolta relativo a ogni server di rapporto in cui il server di gestione è il server padre e ogni server di raccolta è il server figlio.
- Creare una federazione completamente a coppie tra i server di raccolta per ciascun server di rapporto.
- Creare una federazione gerarchica da ciascun server di raccolta al relativo server di rapporto in cui il server di raccolta è il server padre e il server di rapporto è il server figlio.
- Creare una federazione completamente a coppie tra i server di rapporto.

Per soddisfare un determinato obiettivo di rapporti, è importante eseguire il rapporto da un server rappresentato da una posizione particolare sulla mappa della federazione. Ecco alcuni esempi:

- Per generare un rapporto di sistema su eventi di automonitoraggio che si verificano su ogni CA Enterprise Log Manager nella rete, eseguire il rapporto dal server di gestione.
- Per generare rapporti di riepilogo e delle tendenze da tutti i server di rapporto della rete, eseguire il rapporto da qualsiasi server di rapporto.
- Per generare un rapporto sui dati che risiedono in un server di rapporto e nei relativi server di raccolta, eseguire il rapporto da uno di questi server di raccolta.

Esempio: mappa della federazione per un'impresa di medie dimensioni

Prima di creare una mappa della federazione, stabilire il numero di server da dedicare a ciascun ruolo server. Nell'esempio seguente, un server è dedicato alla gestione e ai rapporti e i server restanti sono dedicati alla raccolta. Si consiglia questa configurazione per un ambiente di medie dimensioni. È possibile concepire l'architettura dei server di gestione/rapporto e dei server di raccolta come hub e spoke in cui il server di gestione/rapporto rappresenta l'hub. Il diagramma della mappa della federazione non rispecchia questa configurazione, bensì mostra i livelli in modo da poter facilmente distinguere le coppie federate in modo gerarchico da quelle a coppia.

Quando si crea la mappa di una federazione, considerare i tipi di rapporto per cui si desiderano set diversi di dati consolidati. Ad esempio, considerare lo scenario in cui si desiderano dati consolidati utilizzando tre tipi di raggruppamenti di server:

- Solo il server di gestione/rapporto

  Per la maggior parte dei rapporti in cui si desidera esaminare gli eventi archiviati di recente (warm) evitando che i server di raccolta elaborino le query per i nuovi eventi (hot)

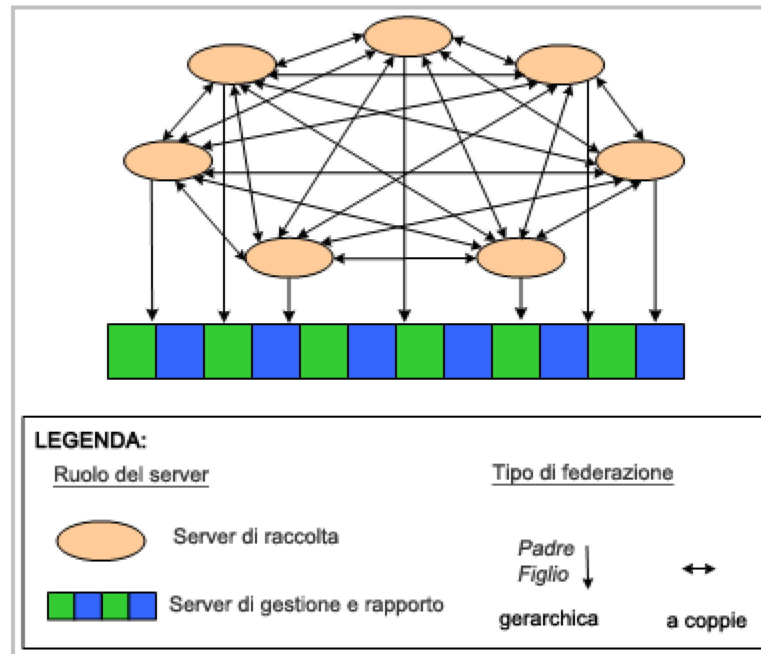
  Nota: gli eventi vengono generalmente archiviati dai server di raccolta (spoke) al server di rapporto (hub) ogni ora.

- Tutti i server

  Per i rapporti di sistema sugli eventi di automonitoraggio in cui si desidera valutare lo stato di tutti i server CA Enterprise Log Manager contemporaneamente

  Per gli avvisi in cui è importare eseguire la query di nuovi eventi da tutti i server di raccolta

A seguire, un esempio di mappa di federazione che permette di soddisfare questi obiettivi dei rapporti:



Per implementare la realizzazione di questa mappa di federazione, è necessario intraprendere le seguenti azioni:

- Creare una federazione completamente a coppie tra i server di raccolta. Ogni server di raccolta è sia padre che figlio per tutti gli altri server di raccolta.
- Creare una federazione gerarchica da ciascun server di raccolta al server di gestione/rapporto in cui il server è il padre e il server di gestione/rapporto è il figlio.

Per raggiungere un determinato obiettivo, è importante eseguire il rapporto o l'avviso da un server rappresentato da una posizione particolare sulla mappa della federazione e specificare correttamente se la federazione è necessaria. Ecco alcuni esempi:

- Per generare un rapporto di sistema sugli eventi di automonitoraggio che si verificano su ogni server CA Enterprise Log Manager nella rete, eseguire il rapporto dal server di gestione/rapporto e specificare la condizione di federazione.
- Per pianificare un rapporto relativo a eventi recenti (warm), eseguire il rapporto dal server d gestione/rapporto e annullare la richiesta per la condizione di federazione. Un rapporto di questo tipo comprende i dati archiviati di recente raccolti da tutti i server di raccolta. La federazione non è necessaria.
- Per pianificare un avviso che comprenda i nuovi eventi (hot) da ciascun server di raccolta e gli eventi archiviati (warm) sul server di gestione/rapporto, eseguire l'avviso da qualsiasi server di raccolta e specificare la condizione di federazione. È possibile limitare i risultati restituiti dai server di raccolta specificando come condizioni dei risultati l'intervallo predefinito, ovvero l'ultima ora trascorsa.

Ulteriori informazioni:

Configurazione di un server CA Enterprise Log Manager come server figlio (a pagina 226)
Ruoli dei server (a pagina 23)
Esempio: archiviazione automatica fra tre server (a pagina 173)

Pianificazione degli utenti e degli accessi

Dopo avere installato il primo server CA Enterprise Log Manager e avere effettuato l'accesso ad esso come utente EiamAdmin, è possibile configurare l'archivio utente, un utente come amministratore e impostare i criteri delle password.

La pianificazione degli utenti e degli accessi è limitata a quanto segue:

- Determinare se accettare l'archivio utente predefinito su questo server CA Enterprise Log Manager o configurare un archivio utente esterno. Se è necessaria una configurazione, registrare i valori richiesti sui fogli di calcolo forniti.
- Identificare l'utente che agirà come primo amministratore. Solo un amministratore può configurare le impostazioni di CA Enterprise Log Manager.
- Definire criteri delle password con l'obiettivo di promuovere password sicure per gli utenti CA Enterprise Log Manager.

  Nota: è possibile configurare criteri delle password solo quando si configura l'archivio utente come archivio utente su questo CA Enterprise Log Manager.

Ulteriori informazioni:

Foglio di calcolo directory LDAP esterna (a pagina 45)
Foglio di lavoro per CA SiteMinder (a pagina 47)

Pianificazione archivio utente

Dopo avere installato il primo server CA Enterprise Log Manager, accedere a CA Enterprise Log Manager e configurare l'archivio utente. L'archivio utente configurato è la posizione in cui vengono conservati nomi utente e password utilizzati per l'autenticazione e altri dettagli globali.

Con tutte le opzioni dell'archivio utente, i dettagli dell'utente dell'applicazione vengono archiviati nell'archivio utente CA Enterprise Log Manager. Questo include informazioni come ruoli, preferiti dell'utente e ora dell'ultimo accesso.

Si deve considerare quanto segue durante la pianificazione dell'archivio utente da configurare:

- Utilizzare l'archivio utente CA Enterprise Log Manager (predefinito)

  Gli utenti vengono autenticati con i nomi utente e le password create in CA Enterprise Log Manager. Configurare i criteri delle password. Gli utenti possono modificare le proprie password e sbloccare gli altri account utente.

- Riferimento da CA SiteMinder

  Nomi utente, password e gruppi globali vengono caricati da CA SiteMinder nell'archivio utente CA Enterprise Log Manager. Gli utenti vengono autenticati con i nomi utente e le password indicati. È possibile assegnare il gruppo globale a un criterio nuovo o a uno esistente. Non è possibile creare nuovi utenti, modificare password o configurare criteri delle password.

- Riferimento dalla directory LDAP (Lightweight Directory Access Protocol)

  I nomi utente e le password sono caricati dalla directory LDAP all'archivio utente CA Enterprise Log Manager. Gli utenti vengono autenticati con i nomi utente e le password indicati. Le informazioni dell'account utente caricato diventano account utente globali. È possibile assegnare agli utenti globali un ruolo utente corrispondente all'accesso che si desidera che essi abbiano in CA Enterprise Log Manager. Non è possibile creare nuovi utenti o configurare criteri delle password.

Importante: Si consiglia di eseguire il backup dei criteri di accesso predefiniti forniti con CA Enterprise Log Manager prima che voi o un amministratore iniziate a lavorare su di essi. Per ulteriori informazioni, vedere *Guida all'amministrazione di CA Enterprise Log Manager*.

Ulteriori informazioni:

Accettare l'Archivio utente predefinito (a pagina 140)
Riferimento a una directory LDAP (a pagina 141)
Riferimento a CA SiteMinder come archivio utente (a pagina 142)

Foglio di calcolo directory LDAP esterna

Prima di fare riferimento a una directory LDAP esterna, raccogliere le seguenti informazioni di configurazione:

Informazioni necessarie	Valore	Commenti
Tipo		Notare il tipo di directory in uso. CA Enterprise Log Manager supporta molte directory diverse inclusa Microsoft Active Directory e Sun ONE Directory. Fare riferimento all'interfaccia utente per un elenco completo delle directory supportate.
Host		Registrare il nome host del server per l'archivio utente o la directory esterna.
Porta		Registrare il numero di porta su cui l'archivio utente esterno o il server della directory è in ascolto. La porta 389 è la porta nota per LDAP (Lightweight Directory Access Protocol). Se il server di registrazione non utilizza la porta 389, registrare il numero di porta corretto.
DN di base		Specificare il nome distintivo (DN) LDAP utilizzato come base. Il DN è un identificativo univoco per una voce nella struttura di una directory LDAP. Nel DN di base non sono consentiti spazi. Solo gli utenti e i gruppi globali rilevati al di sotto di questo DN vengono mappati e ad essi può essere assegnato un gruppo o ruolo di applicazione CA Enterprise Log Manager.
Password		Immettere e confermare la password per l'utente elencato nella riga DN utente.

Informazioni necessarie	Valore	Commenti
DN utente		Immettere credenziali utente valide per ogni utente valido all'interno del registro utente nel cui registro utente è possibile eseguire ricerche. Immettere il nome distintivo (DN) completo dell'utente. È possibile effettuare l'accesso con qualsiasi ID utente con ruolo di amministrazione. Il DN utente e la password associata costituiscono le credenziali utilizzate per il collegamento all'host della directory esterna.
Utilizza Transport Layer Security (TLS)		Specifica se l'archivio utente deve utilizzare il framework TSL per proteggere le trasmissioni di testo in chiaro. Quando selezionato, TLS viene utilizzato nella creazione della connessione LDAP alla directory esterna.
Includi attributi non mappati		Specifica se includere campi non sincronizzati dalla directory LDAP. Gli attributi esterni non mappati possono essere utilizzati per la ricerca e come filtri.
Utenti globali cache		Specifica se conservare gli utenti globali in memoria per l'accesso rapido. La selezione permette ricerche più veloci al costo della scalabilità. Per un piccolo ambiente di prova, la selezione è consigliata.
Orario di aggiornamento cache		Se si è scelto di conservare nella cache gli utenti globali, specificare la frequenza, in minuti, per l'aggiornamento dei gruppi e degli utenti conservati per includere registrazioni nuove e modificate.
Recupera gruppi di scambio come gruppi utenti globali		Se il tipo di directory esterna è Microsoft Active Directory, questa opzione specifica che si intende creare gruppi globali dalle informazioni del gruppo Microsoft Exchange. Se selezionata, è possibile scrivere criteri per i membri degli elenchi di distribuzione.

Foglio di lavoro per CA SiteMinder

Prima di fare riferimento a CA SiteMinder come archivio utente, raccogliere le seguenti informazioni sulla configurazione:

Informazioni necessarie	Valore	Commenti
Host		Definisce nome host o indirizzo IP del sistema CA SiteMinder di riferimento. È possibile utilizzare indirizzi IPv4 o IPv6 IP.
Nome amministratore		Il nome utente per il super utente CA SiteMinder che svolge la manutenzione del sistema e degli oggetti del dominio.
Password amministratore		La password per il nome utente associato.
Nome agente		Il nome dell'agente fornito al server dei criteri. Il nome non distingue tra maiuscole e minuscole.
Segreto agente		Il segreto condiviso che distingue tra maiuscole e minuscole definito in CA SiteMinder. Il nome del segreto agente distingue tra maiuscole e minuscole.
Utenti globali cache		Specifica se conservare nella cache gli utenti globali, permettendo ricerche più rapide al costo della scalabilità. **Nota:** i *gruppi* utenti globali sono sempre posizionati nella cache.
Orario di aggiornamento cache		L'intervallo in minuti dopo cui la cache utente viene aggiornata automaticamente.
Includi attributi non mappati		Specifica se includere gli attributi esterni non mappati per l'utilizzo come filtri o nelle ricerche.
Recupera gruppi di scambio come gruppi utenti globali		Se il tipo di directory esterna è Microsoft Active Directory, questa opzione specifica che si intende creare gruppi globali dalle informazioni del gruppo Microsoft Exchange. Se selezionata, è possibile scrivere criteri per i membri degli elenchi di distribuzione.
Tipo archivio autorizzazione		Definisce il tipo di archivio utente utilizzato.

Informazioni necessarie	Valore	Commenti
Nome archivio autorizzazione		Specifica il nome assegnato dell'archivio utente a cui si fa riferimento nel campo Tipo archivio di autorizzazione.

Utenti con ruolo di amministratore

Solo gli utenti a cui è stato assegnato il ruolo di amministratore possono configurare i componenti CA Enterprise Log Manager.

Dopo l'installazione del primo CA Enterprise Log Manager, si accede a CA Enterprise Log Manager attraverso un browser, si accede con le credenziali EiamAdmin e si configura l'archivio utente.

Il passaggio successivo è l'assegnazione del gruppo applicazione amministratore all'account dell'utente che deve eseguire la configurazione. Se l'archivio utente è stato configurato come archivio utente CA Enterprise Log Manager, quello predefinito, si crea un account utente e si assegna ad esso il ruolo di amministratore. Se si fa riferimento a un archivio utente esterno, non è possibile creare un nuovo utente. In questo caso, si cerca il record utente della persona che deve svolgere il ruolo di amministratore e si aggiunge il gruppo applicazione amministratore a questo account utente.

Pianificazione dei criteri delle password

Se si accetta l'archivio utente predefinito, si definiscono nuovi utenti e si impostano nuovi criteri delle password per questi account utente dall'interno di CA Enterprise Log Manager. L'utilizzo di password complesse aiuta a proteggere le risorse di calcolo. I criteri delle password aiutano nella creazione di password complesse e possono contribuire a impedire l'utilizzo di password deboli.

I criteri delle password predefiniti forniti con CA Enterprise Log Manager offrono una forma molto *leggera* di protezione password. Ad esempio, i criteri predefiniti aiutano gli utenti a utilizzare il proprio nome utente come password e permettono loro di sbloccare le password. Questo consente alle password di non scadere mai e non esegue un blocco in base ai tentativi di accesso falliti. Le opzioni predefinite sono impostate intenzionalmente ad un livello molto basso di sicurezza password per consentire la creazione dei propri criteri delle password personalizzati.

Importante: È necessario modificare i criteri delle password predefiniti per soddisfare le restrizioni delle password in uso presso l'azienda. È sconsigliato eseguire CA Enterprise Log Manager in ambienti di produzione con i criteri delle password predefiniti!

È possibile non permette queste attività, applicare criteri agli attributi delle password come lunghezza, tipo di carattere, età e riutilizzo e stabilire criteri di blocco in base ad un numero configurabile di tentativi di accesso falliti come parte dei criteri delle password personalizzati.

Ulteriori informazioni:

Configurazione dei criteri delle password (a pagina 143)

Nome utente e una password

Affinché le password siano sicure, le migliori prassi di sicurezza suggeriscano di creare password che non contengano o corrispondano al nome utente. Il criterio delle password predefinito abilita questa opzione. Mentre questa opzione sembra utile quando si imposta la password temporanea per i nuovi utenti, è buona prassi cancellare questo criterio di selezione della password. Cancellando questa opzione si impedisce agli utenti di utilizzare questo tipo di password deboli.

Età e riutilizzo delle password

Considerare le seguenti linee guida quando si stabiliscono i criteri di età e riutilizzo:

- I criteri di riutilizzo delle password possono garantire che una determinata password non venga riutilizzata spesso. Questo criterio crea una cronologia delle password. L'impostazione 0 indica che la cronologia delle password non è applicata. Un'impostazione superiore a 0 specifica il numero di password salvate e utilizzate per il confronto quando viene modificata la password. Un criterio delle password sicuro deve impedire agli utenti di riutilizzare una password per almeno un anno.
- L'*età massima* consigliata per una password varia a seconda della lunghezza e della complessità della password. Una regola generale è che una password accettabile è una che non può essere scoperta con attacco di forza bruta in un tempo inferiore all'età massima consentita alla password. Un buono standard di età è da 30 a 60 giorni.
- L'impostazione di un'*età minima* impedisce agli utenti di ripristinare le password molte volte in una singola sessione per aggirare un criterio di riutilizzo della password. Una buona prassi comune consigliata è 3 giorni.

- Se si imposta l'età di una password, si consiglia di avvertire gli utenti di ripristinare le proprie password. È possibile impostare l'avvertimento in modo che si verifichi nel momento centrale dell'età o vicino alla scadenza.
- È necessario bloccare gli account utente dopo un numero ragionevole di accessi non riusciti. Ciò può aiutare a impedire agli hacker di indovinare la password. Da tre a cinque tentativi è il numero massimo standard dopo cui l'account viene chiuso.

Lunghezza e formato della password

Considerare le seguenti linee guida quando si stabilisce se applicare i requisiti della lunghezza:

- A causa del modo in cui le password sono crittografate, le password più sicure sono lunghe sette o 14 caratteri.
- Fare attenzione a non superare i limiti di lunghezza della password imposti da vecchi sistemi operativi nella rete.

Considerare le seguenti linee guida quando si stabilisce se applicare criteri sui caratteri massimi ripetuti o sul numero minimo o sui caratteri numerici.

- Le password sicure non si trovano in nessun dizionario.
- Le password sicure includono uno o più caratteri da almeno tre dei quattro set di lettere minuscole, lettere maiuscole, cifre e caratteri speciali.

Pianificazione aggiornamento sottoscrizioni

CA Enterprise Log Manager viene mantenuto costantemente aggiornato attraverso gli aggiornamenti delle sottoscrizioni forniti dal server di sottoscrizione CA. Gli aggiornamenti delle sottoscrizioni possono contenere alcuni o tutti i seguenti elementi:

- Aggiornamenti del prodotto e del sistema operativo, che vengono installati automaticamente da tutti i server CA Enterprise Log Manager.

  Nota: è possibile scegliere quali aggiornamenti del prodotto e del sistema operativo applicare durante ogni ciclo di aggiornamento.

- Gli aggiornamenti del contenuto e della configurazione, come i seguenti, che vengono inviati al server di gestione.
  - Query dei rapporti
  - Rapporti
  - File di mapping dei dati (DM) e di analisi dei messaggi (XMP)
  - Listener, connettori e altri servizi
  - Integrazioni
  - Aggiornamenti della configurazione dei moduli CA Enterprise Log Manager
  - Aggiornamenti della chiave pubblica
- Aggiornamenti destinati agli agenti

  Nota: aggiornare i propri server CA Enterprise Log Manager prima di eseguire tale operazione sugli agenti. I server CA Enterprise Log Manager supportano gli agenti della loro stessa versione o di quelle inferiori. Per assicurare una corretta archiviazione degli eventi raccolti quando si configurano o si aggiornano agenti, verificare che l'agente invii eventi solo a server CA Enterprise Log Manager, il cui livello è uguale o superiore a quello dell'agente.

Il primo server CA Enterprise Log Manager che si installa è quello predefinito, il proxy di sottoscrizione in linea per gli aggiornamenti delle sottoscrizioni. I server successivi CA Enterprise Log Manager vengono installati come client di sottoscrizione. Se necessario, è possibile configurare qualsiasi server CA Enterprise Log Manager in modo che funzioni come proxy di sottoscrizione *non in linea*. È possibile inoltre configurare proxy di sottoscrizione in linea aggiuntivi.

La pianificazione delle sottoscrizioni implica quanto segue:

- Valutazione della necessità di un proxy HTTP
- Valutazione della necessità di un proxy di sottoscrizione non in linea
- Valutazione della necessità di un elenco di proxy

Componenti e porte di sottoscrizione

La sottoscrizione richiede quanto segue:

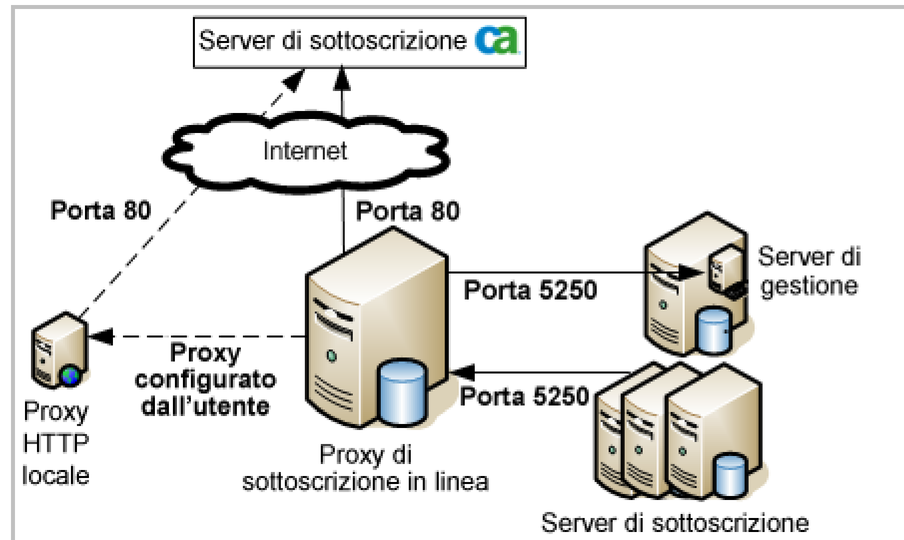
- Il server di sottoscrizione CA
- (Facoltativo) Proxy HTTP
- Ogni server CA Enterprise Log Manager che può essere configurato come uno dei seguenti:
  - Proxy di sottoscrizione (online)
  - Client di sottoscrizione
  - (Facoltativo) Proxy di sottoscrizione non in linea
- Il server CA Enterprise Log Manager di gestione, che tipicamente costituisce il proxy di sottoscrizione predefinito.

  Il primo server CA Enterprise Log Manager installato solitamente viene installato con un CA EEM locale, e il primo CA Enterprise Log Manager installato è, per impostazione predefinita, il proxy di sottoscrizione predefinito.

CA Enterprise Log Manager utilizza un sistema proxy, o client e server, per fornire contenuti e aggiornamenti di file binari. Il primo server CA Enterprise Log Manager che si installa viene impostato automaticamente come proxy di sottoscrizione predefinito. Il proxy di sottoscrizione in linea contatta periodicamente il server di sottoscrizione CA per controllare gli aggiornamenti. Il contatto può essere diretto o attraverso un proxy HTTP. Per impostazione predefinita, tutti gli altri server CA Enterprise Log Manager sono client di sottoscrizione del proxy di sottoscrizione predefinito. I client di sottoscrizione contattano il proxy di sottoscrizione predefinito per gli aggiornamenti. Sia i client che i proxy installano automaticamente i moduli che richiedono.

L'archivio utente CA Enterprise Log Manager riceve aggiornamenti dei contenuti e della configurazione e archivia tutte le configurazioni del servizio di sottoscrizione.

Porta 80, la nota porta del protocollo HTTP, è utilizzata per le richieste a internet attraverso il server di sottoscrizione di CA. La porta 5250 viene utilizzata per il traffico interno tra i server CA Enterprise Log Manager. La porta dal proxy di sottoscrizione in linea al proxy HTTP viene configurata con altre informazioni del proxy HTTP.



Ulteriori informazioni:

Configurazione di un proxy di sottoscrizione in linea (a pagina 195)
Assegnazioni delle porte predefinite (a pagina 112)

Quando configurare la sottoscrizione

È buona prassi rimandare la configurazione della sottoscrizione fin a quando sono installati tutti i server CA Enterprise Log Manager pianificati. Se si preferisce ricevere gli aggiornamenti della sottoscrizione direttamente, considerare di ignorare il valore per la durata della conservazione degli aggiornamenti scaricati rispetto a quello predefinito di 30 giorni, ad un intervallo che permetta a tutti i server CA Enterprise Log Manager pianificati di essere installati e aggiornati prima che venga eseguita la prima cancellazione. Tutti i nuovi server aggiunti come client della sottoscrizione dopo che sono state eseguite una o più cancellazioni non riceveranno gli aggiornamenti resi disponibili prima della cancellazione. Se si installano nuovi server a cancellazione avvenuta, configurarli come proxy di sottoscrizione in modo che tutti gli aggiornamenti disponibili dal server di sottoscrizione di CA possano essere applicati. Dopo che questo avviene, è possibile riconfigurare i nuovi server come client di sottoscrizione.

Pianificazione dello spazio su disco

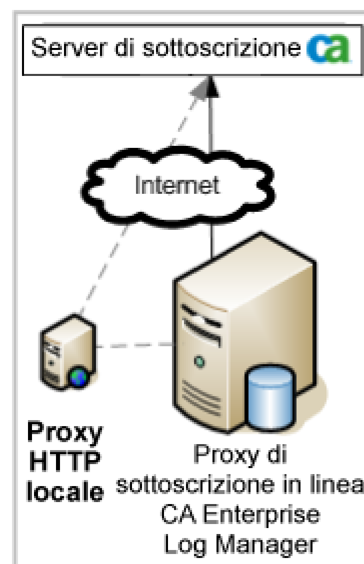
È buona prassi controllare frequentemente lo spazio su disco in modo da poter mantenere spazio adeguato per il download degli aggiornamenti delle sottoscrizioni. Se lo spazio utilizzato su disco di un CA Enterprise Log Manager configurato come client di sottoscrizione supera il 90% quando il motore di aggiornamento tenta di eseguire l'aggiornamento, il servizio di sottoscrizione produce un evento di automonitoraggio e sospende la procedura di download.

È possibile pianificare un avviso di azione in base alla query Spazio su disco insufficiente.

Nota: ad esempio, vedere la sezione *Guida all'amministrazione di CA Enterprise Log Manager* sugli Avvisi azione.

Valutazione della necessità di un proxy HTTP

Prima di configurare le impostazioni delle sottoscrizioni globali, stabilire se si scaricheranno aggiornamenti delle sottoscrizioni nella rete interna attraverso un server proxy HTTP. Molte aziende richiedono che le connessioni internet in uscita siano effettuate attraverso un server proxy HTTP. È possibile specificare le credenziali del server proxy HTTP come parte della configurazione della sottoscrizione. Ciò permette al proxy della sottoscrizione di ignorare il proxy HTTP quando tenta di controllare gli aggiornamenti dal server di sottoscrizione CA. Con il bypass automatico, non è richiesta la presenza di nessuno durante la procedura di aggiornamento della sottoscrizione.



Se si utilizza un proxy HTTP, è necessario disporre dell'indirizzo IP, del numero della porta e delle credenziali quando si avvia questa configurazione.

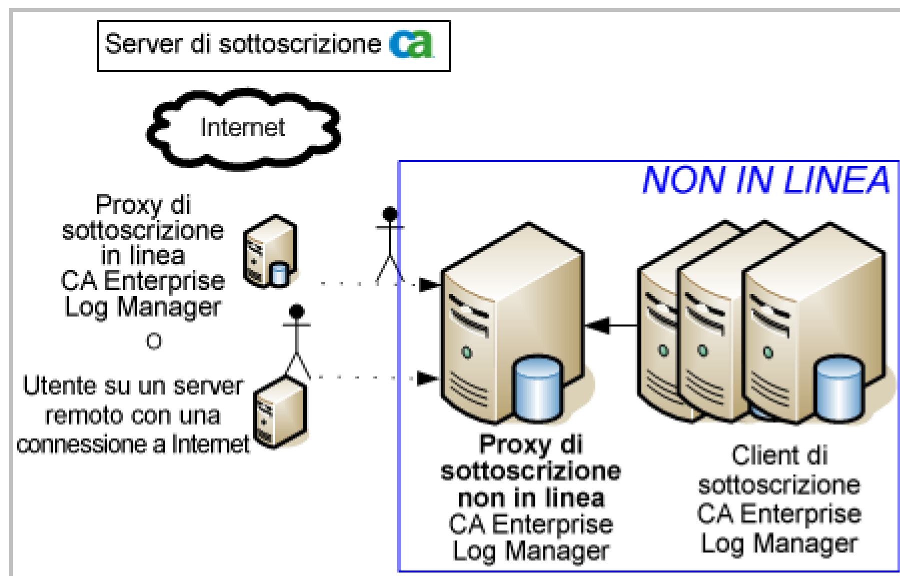
Verifica dell'accesso a Feed RSS per la sottoscrizione

Quando si iniziano a configurare impostazioni di sottoscrizione globali, verificare che il server proxy di sottoscrizione predefinito possa accedere all'URL del Feed RSS. Se i moduli disponibili per scaricare gli elenchi sono popolati, questo indica un accesso riuscito.

Se l'area dei moduli di download disponibili non è popolata e il server si trova dietro a un firewall, assicurarsi di configurare le impostazioni del proxy HTTP, in modo che i proxy online possano contattare il Feed RSS.

Valutazione della necessità di un proxy di sottoscrizione non in linea

Prima di configurare la sottoscrizione, stabilire quando si devono designare i proxy di sottoscrizione non in linea. La necessità di proxy di sottoscrizione non in linea si verifica quando i server CA Enterprise Log Manager configurati come client di sottoscrizione non hanno accesso ai proxy di sottoscrizione in linea a causa di criteri che non autorizzano questi server ad accedere a qualsiasi server con accesso a internet. I criteri potrebbero addirittura essere tali che nessun server CA Enterprise Log Manager possa costituire un proxy di sottoscrizione in linea. In entrambi i casi, è necessario un proxy di sottoscrizione non in linea. La differenza tra questi scenari è la modalità di recupero degli aggiornamenti delle sottoscrizioni dal server di sottoscrizione di CA; in un caso, gli aggiornamenti vengono recuperati su base pianificata da un proxy online; nell'altro caso, gli aggiornamenti vengono ripristinati manualmente da un individuo presso un server remoto.



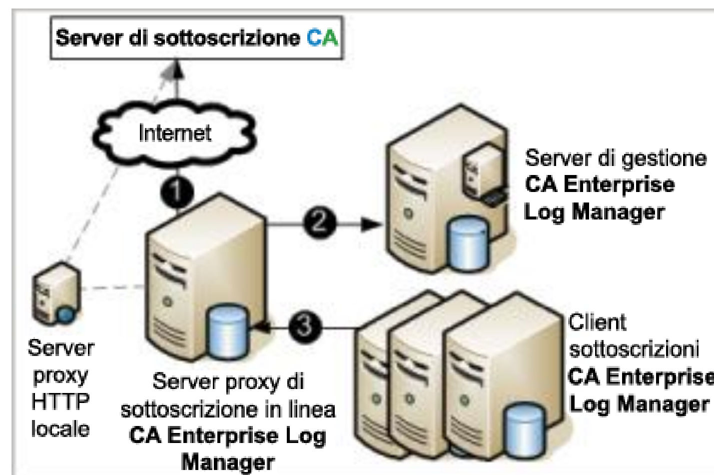
Ulteriori informazioni:

Configurazione di un proxy di sottoscrizione non in linea (a pagina 197)

Funzionamento della sottoscrizione con client in linea

Il proxy di sottoscrizione in linea predefinito e altri proxy di sottoscrizione che vengono configurati ricevono gli aggiornamenti delle sottoscrizioni dal server di sottoscrizione CA. Essi effettuano il bypass di un server proxy HTTP, se configurato.

La seguente illustrazione raffigura un semplice scenario online con il server di sottoscrizione CA, il proxy di sottoscrizione in linea predefinito, il server di gestione CA Enterprise Log Manager e alcuni client di sottoscrizione:



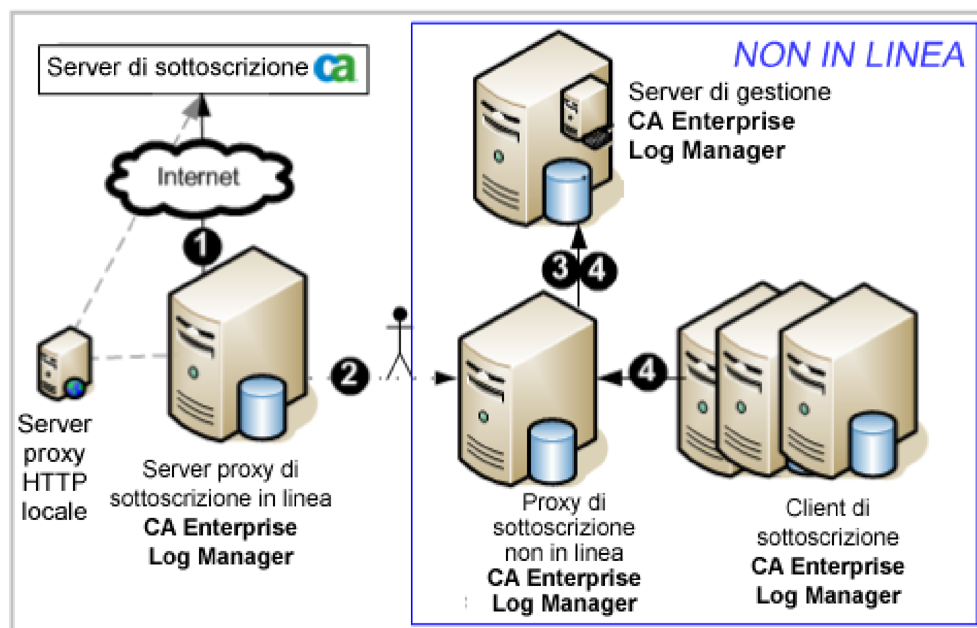
Di seguito si trova una descrizione del processo mostrato dalle frecce numerate:

1. Quando l'amministratore esegue la messa a punto iniziale di "Configurazione di servizio globale: modulo di sottoscrizione" e specifica l'URL del feed RSS, il proxy di sottoscrizione accede al server di sottoscrizione di CA attraverso l'URL del feed RSS per ottenere l'elenco dei moduli disponibili per il download. Quando l'amministratore seleziona i moduli da scaricare, il sistema stabilisce quali aggiornamenti non sono ancora stati scaricati sul proxy online. Il proxy di sottoscrizione in linea scarica nuovi aggiornamenti delle sottoscrizioni, probabilmente attraverso un server proxy HTTP locale. Gli aggiornamenti delle sottoscrizioni includono aggiornamenti dei contenuti e aggiornamenti del prodotto e del sistema operativo.

2. Il proxy di sottoscrizione in linea invia gli aggiornamenti di contenuto e configurazione al componente server di gestione CA Enterprise Log Manager che archivia questo tipo di informazioni per tutti i CA Enterprise Log Manager all'interno dell'ambiente.
3. I client di sottoscrizione eseguono il polling del server proxy di sottoscrizione. Se sono disponibili nuovi aggiornamenti, i client di sottoscrizione li scaricano. Il download consiste in un file zip contenente gli aggiornamenti del prodotto e del sistema operativo, uno script per installarli e un file delle informazioni sul componente (componentinfo.xml). Se bisogna eseguire un backup, i client di sottoscrizione creano un backup dell'installazione più recente degli aggiornamenti di prodotto ed uno script per ripristinare lo stato degli aggiornamenti, nel caso occorra eseguire un ripristino alla versione precedente delle modifiche. (Il backup non comprende gli aggiornamenti del sistema operativo.) Quindi, i client di sottoscrizione eseguono lo script che installa gli aggiornamenti di prodotto.

Funzionamento della sottoscrizione con client non in linea

La seguente illustrazione mostra un semplice scenario non in linea con il server di sottoscrizione CA, il proxy di sottoscrizione in linea predefinito, un proxy di sottoscrizione non in linea, un server di gestione con l'archivio utente CA Enterprise Log Manager e alcuni client di sottoscrizione.



Di seguito si trova il processo rappresentato dalle frecce numerate:

1. Il proxy di sottoscrizione in linea accede al server di sottoscrizione CA e scarica aggiornamenti di contenuti e aggiornamenti del prodotto e del sistema operativo, probabilmente attraverso un server HTTP locale. Gli aggiornamenti di prodotto scaricati si basano sui moduli selezionati da scaricare, configurati come parte di Configurazione dei servizi globali: modulo di sottoscrizione.

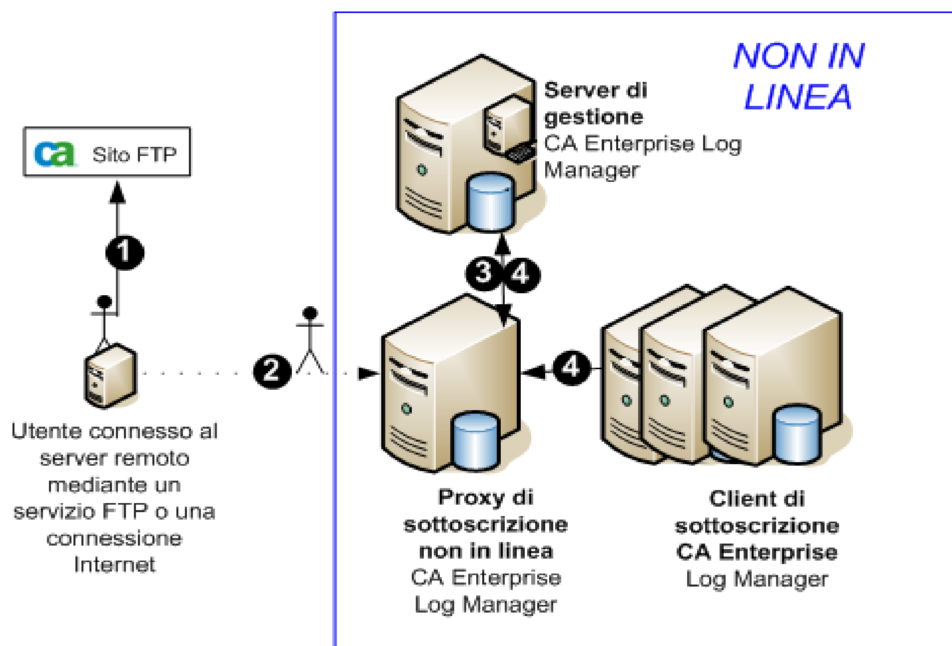
2. Si copia ogni elemento presente nel percorso di download del proxy online nel percorso di download del proxy non in linea. L'utilità *scp* (copia di sicurezza) viene fornita a questo scopo. È inoltre possibile utilizzare sftp. Il contenuto copiato include gli aggiornamenti dei contenuti e aggiornamenti binari del prodotto e del sistema operativo. Dopo la copia, modificare la proprietà dei file all'utente caelmservice.

3. Il server proxy di sottoscrizione non in linea invia gli aggiornamenti dei contenuti al server di gestione CA Enterprise Log Manager.

4. I client di sottoscrizione eseguono il polling del server proxy di sottoscrizione *non in linea*. Se sono disponibili nuovi aggiornamenti, i client di sottoscrizione li scaricano. Il download consiste in un file zip contenente gli aggiornamenti del prodotto e del sistema operativo, uno script per installarli e un file delle informazioni sul componente (componentinfo.xml). Se bisogna eseguire un backup, i client di sottoscrizione creano un backup dell'installazione più recente degli aggiornamenti di prodotto ed uno script per ripristinare lo stato degli aggiornamenti, nel caso occorra eseguire un ripristino alla versione precedente delle modifiche. (Il backup non comprende gli aggiornamenti del sistema operativo.) Quindi, i client di sottoscrizione eseguono lo script che installa gli aggiornamenti di prodotto.

Funzionamento della sottoscrizione senza proxy in linea

È possibile eseguire un sistema di server CA Enterprise Log Manager in cui nessun server dispone di accesso a internet. In questa eccezione, anche il primo server installato, che viene configurato automaticamente come il proxy di sottoscrizione predefinito, non dispone di accesso in linea. È possibile configurare il proxy di sottoscrizione predefinito come un proxy non in linea. Per ottenere gli aggiornamenti, è necessario accedere manualmente al sito FTP di CA specificato. Il sito FTP contiene una cartella per ogni versione principale. Le cartelle di versioni precedenti, come r12.0, contengono un file core tar contenente la versione, i service pack e gli aggiornamenti aggiunti durante il ciclo di rilascio. La cartella della versione corrente contiene un file core, aggiornato con tutti i service pack, e un file aggiuntivo contenente gli aggiornamenti cumulativi gli aggiornamenti rapidi. È possibile ottenere il file tar desiderato tramite FTP da qualsiasi server nella rete dell'utente. per ottenerlo, estrarre il file nel percorso di download del server proxy non in linea. L'aggiornamento del repository del contenuto e dei client procede come configurato.



Di seguito si trova il processo rappresentato dalle frecce numerate:

1. Da un server remoto con una connessione Internet o un servizio FTP in esecuzione, accedere al sito FTP contenente un file tar per ogni versione e Service pack di CA Enterprise Log Manager. Aprire la cartella della versione corrente o della versione desiderata. Scaricare il file core subscription_12.x.x.x.tar, qualora non sia stato precedentemente scaricato. Se il file è già stato scaricato, scaricare il file aggiuntivo.
2. Inserire il percorso di download del proxy non in linea con gli aggiornamenti:
   a. Se è stato scaricato il file tar core, copiare il file nella directory del proxy non in linea /opt/CA/LogManager/data. L'utilità scp (copia di sicurezza) viene fornita a questo scopo. È inoltre possibile utilizzare sftp.
   b. Rinominare la directory di sottoscrizione esistente in subscription.bak
   c. Estrarre il file tar.

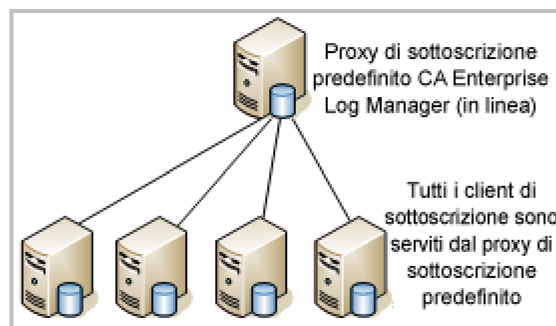
      ```
      tar -xvf subscription_x_x_x_x.tar
      ```

      La struttura di directory /opt/CA/LogManager/data/subscription viene creata con il contenuto e i file binari più recenti. Le autorizzazioni e la proprietà sono state impostate.
   d. Se è stato scaricato il file tar aggiuntivo, copiare il file nella directory del proxy non in linea /opt/CA/LogManager/data/subscription ed estrarlo. Questa procedura consente di aggiornare i moduli e i file con le versioni più recenti.
   e. Riavviare il servizio iGateway.
3. Il server proxy di sottoscrizione non in linea invia gli aggiornamenti dei contenuti al repository del server di gestione CA Enterprise Log Manager.
4. I client di sottoscrizione, inclusi il client sul server di gestione e il proxy non in linea, eseguono il polling del server proxy di sottoscrizione *non in linea* per gli aggiornamenti. Se sono disponibili nuovi aggiornamenti, i client di sottoscrizione li scaricano. Il download consiste in un file zip contenente gli aggiornamenti del prodotto e del sistema operativo, uno script per installarli e un file delle informazioni sul componente (componentinfo.xml). Se è necessario eseguire un backup, i client di sottoscrizione creano una backup dell'ultima installazione di aggiornamenti del prodotto e uno script di rollback delle modifiche. (Il backup non include gli aggiornamenti del sistema operativo.) Quindi, i client di sottoscrizione eseguono lo script di installazione che installa gli aggiornamenti del prodotto.

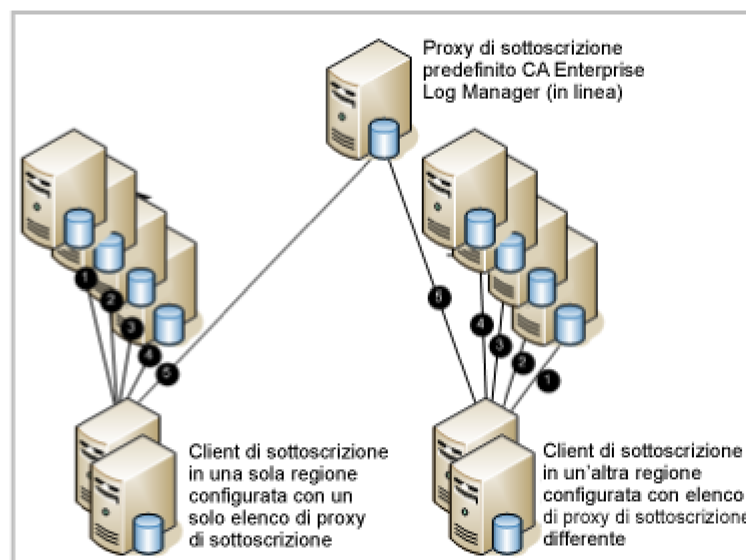
Valutazione della necessità di un elenco di proxy

Prima di configurare i client di sottoscrizione, stabilire la fonte da cui essi recuperano gli aggiornamenti dei contenuti. I client di sottoscrizione possono ricevere gli aggiornamenti direttamente dal proxy di sottoscrizione predefinito oppure è possibile configurare un elenco intermedio di proxy per ridurre il carico delle richieste di aggiornamento.

- Per aziende con solo pochi server CA Enterprise Log Manager a stretto contatto nella rete, si consiglia di fare utilizzare a tutti i client il proxy di sottoscrizione predefinito.



- Per aziende con un gran numero di server CA Enterprise Log Manager o in cui i server CA Enterprise Log Manager sono ampiamente sparsi, si consiglia di configurare un elenco di proxy di sottoscrizione per ogni client di sottoscrizione. Quando viene configurato un elenco di proxy, ogni client contatta i membri di un elenco di proxy, uno per volta, e solo se non ha successo contatta il proxy di sottoscrizione predefinito.



Esempio: configurazione della sottoscrizione con sei server

Quando si procede alla configurazione della sottoscrizione, considerare gli altri ruoli svolti dai server prima di decidere il loro ruolo di sottoscrizione. Per impostazione predefinita il server di gestione, il primo server che si installa, è il proxy di sottoscrizione predefinito. Tutti gli altri server sono client di sottoscrizione del proxy di sottoscrizione predefinito. Anche se questo è accettabile, è preferibile configurare un proxy di sottoscrizione in linea e fare operare il proxy predefinito come proxy failover o ridondante. È buona prassi assegnare il ruolo di proxy in linea al server meno attivo.

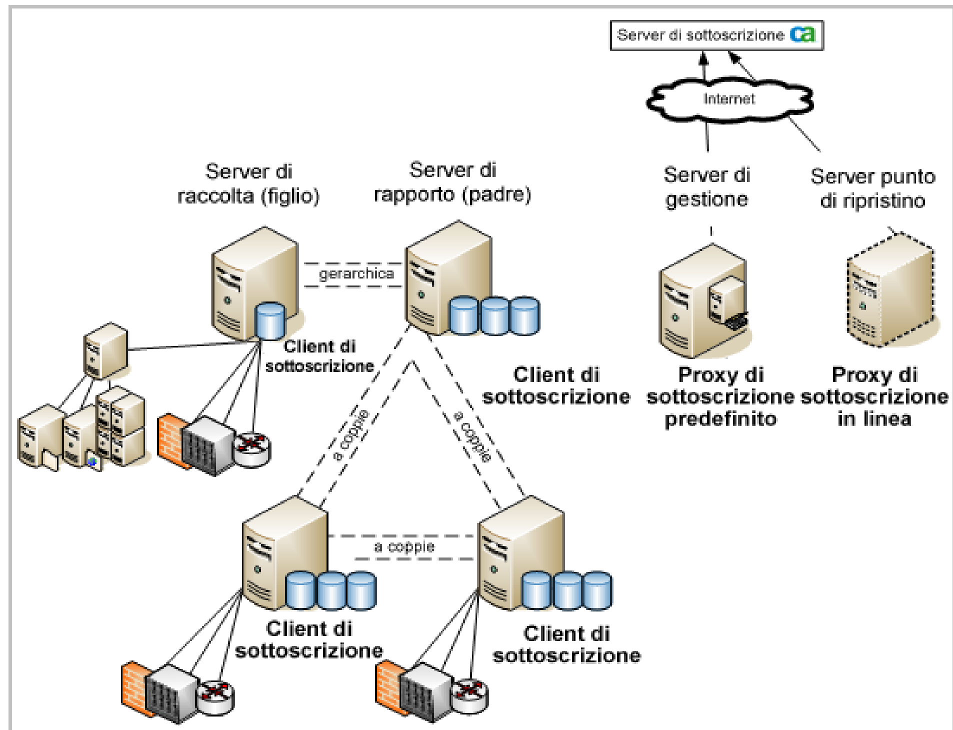
Esempio: sei server di cui il server meno occupato è il proxy di sottoscrizione in linea

Considerare uno scenario di sei server CA Enterprise Log Manager. Il server di gestione è dedicato all'autenticazione e all'autorizzazione degli utenti all'accesso e all'archiviazione del contenuto delle applicazioni. Quattro server federati gestiscono l'elaborazione e i rapporti di eventi. Un sesto server costituisce un punto di ripristino dedicato per l'analisi degli eventi dai database ripristinati. Uno dei vantaggi di un punto di ripristino dedicato è che è possibile impedire l'inclusione dei dati vecchi nei rapporti correnti non includendo questo server nella federazione.

In questo esempio, i due server di raccolta e rapporto rappresentano una configurazione con requisiti di elaborazione particolarmente elevati. Questi server sono federati in una configurazione gerarchica, in cui il server di raccolta è figlio del server di notifica. I due server che agiscono come server di raccolta e rapporto rappresentano una configurazione con volumi di eventi normali e rapporti pianificati. Sono federati tra loro e il server dei rapporti dedicato in una federazione a coppie, ossia i tre server sono peer. Lo scopo della federazione di server è estendere la possibilità di ricevere risultati delle query dai server federati. Una query federata da ognuno di questi server a coppie restituisce eventi da se stessa e dagli altri tre server della federazione.

Nota: per eseguire rapporti consolidati su eventi di automonitoraggio, includere il server di gestione nella federazione.

In questo scenario, si consiglia di configurare il punto di ripristino come proxy di sottoscrizione in linea, poiché si tratta del server meno attivo. Quindi configurare ogni client per puntare a questo proxy in linea, in modo che il proxy predefinito possa agire come backup, nel caso il proxy in linea dovesse essere occupato o non disponibile.



Ulteriori informazioni:

Configurazione di una federazione CA Enterprise Log Manager (a pagina 225)
Configurazione di server CA Enterprise Log Manager per la sottoscrizione (a pagina 194)
Ruoli dei server (a pagina 23)

Pianificazione agente

Gli agenti usano connettori per raccogliere gli eventi e trasportarli al server CA Enterprise Log Manager. È possibile configurare un connettore sull'agente predefinito installato con il server CA Enterprise Log Manager oppure è possibile installare un agente su un server o una fonte di eventi nella rete. La decisione di utilizzare agenti esterni si basa sul volume di eventi, sulla posizione dell'agente, sulle esigenze di filtraggio di eventi e su altre considerazioni. La pianificazione dell'installazione di un agente implica quanto segue:

- Comprensione delle relazioni tra i seguenti componenti:
  - Integrazioni e listener
  - Agenti
  - Connettori
- Dimensionamento della rete per decidere quanti agenti installare

È necessario installare gli agenti relativamente vicino alle fonti degli eventi da cui si desidera raccogliere i registri eventi. La maggior parte dei connettori raccoglie eventi da una e un'unica fonte di eventi. Per gli eventi syslog, un unico listener syslog può ricevere eventi da diversi tipi di fonti di eventi. Un agente può controllare e gestire il traffico degli eventi per più di un connettore.

Informazioni sulla raccolta di eventi syslog

CA Enterprise Log Manager può ricevere eventi direttamente da fonti syslog. La raccolta di syslog si differenzia dagli altri metodi di raccolta perché molte fonti di registri diverse possono inviare eventi a CA Enterprise Log Manager contemporaneamente. Considerare un router di rete e un concentratore VPN come due possibili fonti di eventi. Entrambi possono inviare eventi direttamente a CA Enterprise Log Manager utilizzando syslog, ma i formati del registro e le strutture sono diversi. Un agente syslog può ricevere entrambi i tipi di eventi allo stesso tempo utilizzando il listener syslog fornito.

In linea di massima, la raccolta di eventi rientra in due categorie:

- CA Enterprise Log Manager è *in ascolto* per gli eventi syslog su porte configurabili.
- CA Enterprise Log Manager esegue il *monitoraggio* di altre fonti di eventi per i loro eventi, ad esempio, utilizzando WMI per raccogliere eventi di Windows.

Più di una fonte di eventi syslog può trasmettere eventi attraversi un unico connettore, poiché il listener riceve tutto il traffico su una porta specifica. CA Enterprise Log Manager può essere in ascolto per eventi syslog su ogni porta (se si sta eseguendo un agente come utente non principale possono essere presenti limitazioni sull'utilizzo delle porte inferiori alla porta 1024). Le porte standard possono ricevere un flusso di eventi composto da molti tipi diversi di eventi syslog. Essi possono includere UNIX, Linux, Snort, Solaris, CiscoPIX, Check Point Firewall 1 e altri. CA Enterprise Log Manager gestisce gli eventi syslog utilizzando listener che costituiscono un tipo specializzato di componente di integrazione. Si realizzano connettori syslog in base ai listener e alle integrazioni:

- Il listener fornisce informazioni sulla connessione come porte oppure host sicuri.
- L'integrazione definisce i file di analisi dei messaggi (XMP) e di mapping dei dati (DM).

Poiché un unico connettore syslog può ricevere eventi da molte fonti di eventi, si deve considerare se instradare gli eventi syslog in base al loro tipo o fonte. La dimensione e la complessità dell'ambiente determina come bilanciare la ricezione degli eventi syslog:

Molti tipi syslog: 1 connettore

Se un unico connettore deve elaborare eventi da diverse fonti syslog e il volume di eventi è elevato, il connettore deve analizzare tutte le integrazioni applicate (file XMP) fino a quando rileva una corrispondenza per un evento. Questo può provocare un rallentamento delle prestazioni poiché la quantità di dati da elaborare è molto più elevata. Tuttavia, se il volume di eventi non è troppo elevato, un unico connettore sull'agente predefinito potrebbe essere sufficiente per raccogliere tutti gli eventi richiesti per l'archiviazione.

1 tipo syslog: 1 connettore

Se si configura una serie di connettori singoli per elaborare eventi da un unico tipo syslog, è possibile snellire il carico di elaborazione distribuendolo su diversi connettori. Tuttavia, anche avere troppi connettori in esecuzione su un unico agente può ridurre le prestazioni, poiché ognuno corrisponde a un'istanza separata che richiede un'elaborazione individuale.

Alcuni tipi syslog: 1 connettore

Se l'ambiente ha un volume di eventi più consistente per alcuni tipi di eventi syslog, è possibile configurare un connettore per raccogliere solo tale tipo. Quindi è possibile configurare uno o più connettori diversi per raccogliere più di un tipo di eventi syslog con un volume di eventi inferiore nell'ambiente. In questo modo, è possibile bilanciare il carico della raccolta degli eventi syslog su un numero inferiore di connettori garantendo prestazioni migliori.

Non si devono necessariamente creare listener syslog personalizzati, anche se è possibile farlo se necessario. È possibile creare listener syslog personalizzati con valori predefiniti per porte, host sicuri e altro ancora. Ciò può aiutare a semplificare la creazione di connettori se si dispone di molti connettori da creare per ogni tipo di evento syslog, ad esempio.

Ulteriori informazioni:

Account utente predefinito (a pagina 110)
Assegnazioni delle porte predefinite (a pagina 112)
Reindirizzamento delle porte del firewall per gli eventi syslog (a pagina 117)

Agenti e certificati degli agenti

Il certificato CAELM_AgentCert.cer viene utilizzato da tutti gli agenti per comunicare con il server CA Enterprise Log Manager.

Se si sceglie di sostituire il certificato con un certificato personalizzato, è consigliabile eseguire l'operazione prima di installare gli agenti. Se si implementa un certificato personalizzato dopo l'installazione e la registrazione degli agenti con un server CA Enterprise Log Manager, è necessario disinstallare ciascun agente, eliminare la voce dell'agente in Gestione agenti, reinstallare l'agente e riconfigurare i connettori.

Informazioni sugli agenti

Gli agenti vengono eseguiti come servizio o daemon dopo l'installazione e sono componenti opzionali del prodotto, utilizzati in una o più delle seguenti situazioni:

- Un piccolo sito remoto richiede la raccolta di dati degli eventi, ma non richiede un dispositivo software CA Enterprise Log Manager completo.
- È necessario filtrare i dati alla fonte dell'evento per ridurre il traffico di rete o la quantità di dati archiviati.
- È necessario garantire la consegna degli eventi all'archivio registro eventi per la conformità.
- È necessaria una trasmissione dei registri sicura all'interno della rete con crittografia dei dati.

Gli agenti operano come gestori dei processi per i connettori che raccolgono dati degli eventi da applicazioni specifiche, sistemi operativi o database. Gli agenti forniscono comandi di gestione dei connettori come avvio, interruzione e riavvio dall'interfaccia dell'Explorer agente in CA Enterprise Log Manager. Gli agenti applicano anche modifiche alla configurazione dei connettori e aggiornamenti dei file binari.

È possibile installare agenti su singole fonti di eventi oppure è possibile installare agenti su server di host remoti per raccogliere gli eventi da più di una fonte di eventi. L'installazione del server CA Enterprise Log Manager installa automaticamente il proprio agente. È possibile utilizzare questo agente predefinito per la raccolta diretta degli eventi syslog.

È possibile inoltre visualizzare lo stato di ogni agente dall'Explorer agente in ogni server CA Enterprise Log Manager nella rete. Gli agenti hanno un servizio di controllo che riavvia un agente nel caso si blocchi in modo imprevisto e che esegue il monitoraggio degli aggiornamenti dei file binari di agenti e connettori. Gli agenti inviano anche eventi di automonitoraggio all'archivio registro eventi per il tracciamento delle modifiche e dello stato.

Informazioni sui gruppi di agenti

È possibile anche creare gruppi di agenti, che sono raggruppamenti logici di agenti che facilitano la loro gestione. Dopo avere reso un agente parte di un gruppo di agenti, è possibile modificare configurazioni e avviare e interrompere tutti i connettori in un gruppo allo stesso momento. Ad esempio, si potrebbe decidere di raggruppare gli agenti in base alla regione fisica e geografica.

È possibile creare gruppi e spostare gli agenti tra i gruppi nell'Explorer agente. Se non si definisce un gruppo di agenti, tutti gli agenti risiederanno nel gruppo predefinito creato durante l'installazione di CA Enterprise Log Manager.

Le configurazioni degli agenti e i registri dei gruppi di agenti vengono archiviati nel server di gestione. Ogni volta che si installa un agente, il server di gestione rende disponibile il nuovo agente nell'Explorer agente per ogni server CA Enterprise Log Manager che ha registrato con lo stesso nome di istanza dell'applicazione. Ciò permette di configurare e controllare qualsiasi agente da ogni server CA Enterprise Log Manager all'interno della rete.

Privilegi dell'account utente dell'agente

Gli agenti possono essere eseguiti con account utente a basso privilegio. È necessario creare un gruppo e un account utente di servizio nell'host di destinazione prima di installare un agente. Si dovrà specificare il nome utente durante l'installazione dell'agente e il programma di installazione imposterà correttamente le autorizzazioni. Su sistemi Linux, l'utente dell'agente possiede tutti i file binari dell'agente, eccetto i file binari del controllo di proprietà dell'utente principale.

Informazioni sulle integrazioni

Il set di integrazioni pronte all'uso consiste essenzialmente in una libreria di modelli. Questi modelli forniscono il codice specifico per la raccolta di eventi da un tipo particolare di fonte di registri. Un'integrazione diventa un connettore quando viene presa dalla libreria, configurata e applicata alla fonte dell'evento. Le integrazioni contengono i seguenti tipi di informazioni:

- File di accesso ai dati con informazioni per un tipo particolare di fonte degli eventi
- File di analisi dei messaggi che creano coppie nome-valore dai registri eventi raccolti
- File di mapping dei dati che mappano le coppie nome-valore analizzate nella grammatica evento comune che forma lo schema del database per l'archivio registro eventi del server CA Enterprise Log Manager

CA Enterprise Log Manager fornisce una serie di integrazioni per fonti di eventi note e comuni inclusi prodotti CA, firewall noti, database, sistemi operativi, applicazioni e altro ancora. È possibile ricevere le integrazioni aggiuntive nei seguenti modi:

- Aggiornamenti delle sottoscrizioni che includono nuove integrazioni o nuove versioni di quelle esistenti
- Creazione di integrazioni personalizzate utilizzando la procedura guidata fornita

Si utilizzano le integrazioni per specificare il tipo di raccolta eventi che si vuole eseguire quando si configurano i connettori.

Informazioni sui connettori

I connettori ascoltano gli eventi e periodicamente inviano eventi dello stato all'agente per il trasporto al server CA Enterprise Log Manager. Un *connettore* è un processo che utilizza un sensore di registro e un'integrazione per creare una configurazione per la raccolta di eventi da un tipo particolare di fonte di eventi. Diversamente da syslog, un connettore utilizza un'integrazione come modello della propria configurazione. I connettori syslog si basano sui listener.

Gli agenti utilizzano connettori per raccogliere gli eventi. Dopo avere installato un agente è possibile utilizzare l'Explorer agente su ogni server CA Enterprise Log Manager per configurare uno o più connettori su tale agente (i server CA Enterprise Log Manager devono essere registrati nello stesso server di gestione (o server CA EEM esterno) e con lo stesso nome di istanza dell'applicazione per configurare gli agenti in questo modo).

Generalmente esiste un connettore per ogni fonte di evento nella rete. Per gli eventi syslog, può essere presente più di un connettore per molte fonti di eventi, a seconda delle scelte della configurazione. È possibile creare diversi connettori che utilizzano la stessa integrazione, ma che hanno dettagli di configurazione leggermente diversi per accedere alle diverse fonti degli eventi. Alcuni connettori offrono assistenti della configurazione che raccolgono le informazioni necessarie per l'accesso alla fonte dell'evento. Se è necessario un connettore per cui al momento non è fornita un'integrazione, è possibile crearla utilizzando l'integrazione guidata.

Informazioni sui sensori di registro

Un *sensore di registro* è il componente di un connettore che comprende come accedere alle fonti degli eventi. CA Enterprise Log Manager fornisce sensori di registro per i seguenti tipi diversi di fonti di evento e formati di registro:

ACLogsensor

Questo sensore di registro legge gli eventi CA Access Control quando CA Access Control utilizza selogrd per il routing di eventi.

FileLogSensor

Questo sensore di registro legge gli eventi da un file.

LocalSyslog

Questo sensore di registro raccoglie gli eventi dai file syslog locali di qualsiasi server UNIX.

ODBCLogSensor

Questo sensore di registro utilizza ODBC per connettersi a una fonte di eventi di database e recuperare gli eventi da esso.

OPSECLogSensor

Questo sensore di registro legge gli eventi da una fonte di eventi Check Point OPSEC.

SDEELogSensor

Questo sensore di registro legge gli eventi da dispositivi Cisco.

Syslog

Questo sensore di registro è in ascolto per eventi syslog.

TIBCOLogSensor

Questo sensore di registro legge gli eventi da una coda del servizio messaggi di evento (EMS, Event Message Service) TIBCO nelle implementazioni CA Access Control.

W3CLogSensor

Questo sensore di registro legge gli eventi da un file in formato registro W3C.

WinRMLinuxLogSensor

Questo sensore di registro consente all'agente predefinito (Linux) sul server CA Enterprise Log Manager di raccogliere gli eventi Windows.

WMILogSensor

Questo sensore di registro raccoglie gli eventi da origini eventi Windows utilizzando Windows Management Instrumentation (WMI).

Altri sensori di registro possono essere resi disponibili attraverso aggiornamenti della sottoscrizione. Ulteriori informazioni sulla configurazione dei sensori di registro sono disponibili nella guida online e nella *Guida di amministrazione*.

Dimensionamento della rete CA Enterprise Log Manager

Quando si pianifica il numero degli agenti necessari, è possibile utilizzare un semplice schema di ridimensionamento come il seguente. Primo, determinare il numero di connettori necessari. Non è necessario installare un agente su ogni fonte di evento. Sarà tuttavia necessario configurare un connettore per ogni origine evento diversa da syslog da cui si pianifica di raccogliere eventi. È possibile raccogliere gli eventi WMI da più origini eventi su un solo connettore aggiungendo un sensore di registro per ogni origine eventi. Tenere conto dei volumi degli eventi aggregati quando si configura un connettore in questo modo.

È possibile configurare i connettori syslog in diversi modi. Ad esempio, è possibile configurare un singolo connettore syslog per ricevere tutti gli eventi syslog a prescindere dal tipo. Tuttavia, è una buona prassi basare i connettori syslog sui volumi di eventi da specifiche origini eventi syslog.

È possibile installare gli agenti su un'origine eventi individuale. Si consiglia questo approccio quando il conteggio degli eventi da tale origine è elevato. Il piano deve includere una distinzione tra gli agenti in un'origine eventi e gli agenti in un host che opera come raccoglitore di diversi tipi di eventi.

Effetti della regola di soppressione

Durante la pianificazione, è consigliabile riflettere sugli effetti delle *regole di soppressione*, che impediscono agli eventi di essere inseriti nell'archivio registro eventi o di essere raccolti da un connettore. Le regole di soppressione sono sempre collegate a un connettore. È possibile applicare regole di soppressione a livello di agente o gruppo, oppure al server CA Enterprise Log Manager stesso. Gli effetti differiscono in base alla posizione:

- Le regole di soppressione applicate a livello dell'agente o del gruppo impediscono agli eventi di essere raccolti, riducendo quindi l'importo del traffico di rete *inviato* al server CA Enterprise Log Manager.
- Le regole di soppressione applicate al server CA Enterprise Log Manager impediscono agli eventi di essere *inseriti* nel database, riducendo quindi la quantità di informazioni archiviate.

Occorre fare delle considerazioni sulle prestazioni potenziali derivanti dall'applicazione delle regole di soppressione agli eventi dopo il loro arrivo sul server CA Enterprise Log Manager, in particolare se si creano più regole di soppressione o se la velocità del flusso degli eventi è elevata.

Ad esempio, è consigliabile eliminare *alcuni* eventi da un firewall o da alcuni server Windows che producono eventi duplicati per la stessa azione. La mancata raccolta di questi eventi può velocizzare il trasferimento dei registri evento che si desidera mantenere e far risparmiare tempo per l'elaborazione sul server CA Enterprise Log Manager. In casi simili, applicare una o più regole di soppressione adeguate ai componenti degli agenti.

Se si desidera eliminare tutti gli eventi di un certo tipo da più piattaforme o nell'intero ambiente, applicare una o più regole di soppressione adeguate sul server CA Enterprise Log Manager. La valutazione degli eventi in merito alla soppressione si verifica quando gli eventi arrivano al server CA Enterprise Log Manager. L'applicazione di un vasto numero di regole di soppressione al server può portare a un rallentamento delle prestazioni, poiché il server deve applicare le regole di soppressione oltre a inserire gli eventi nell'archivio registro eventi.

Per le implementazioni più piccole, la soppressione può essere eseguita sul server CA Enterprise Log Manager. Si può anche scegliere di applicare la soppressione sul server per le distribuzioni in cui è in uso il riepilogo (aggregazione). Se si stanno inserendo soltanto alcuni degli eventi da un'origine che genera grandi quantità di informazioni, si può sempre scegliere di eliminare gli eventi indesiderati a livello di agente o di gruppo di agenti per risparmiare tempo per l'elaborazione sul server CA Enterprise Log Manager.

Capitolo 3: Installazione di CA Enterprise Log Manager

Questa sezione contiene i seguenti argomenti:

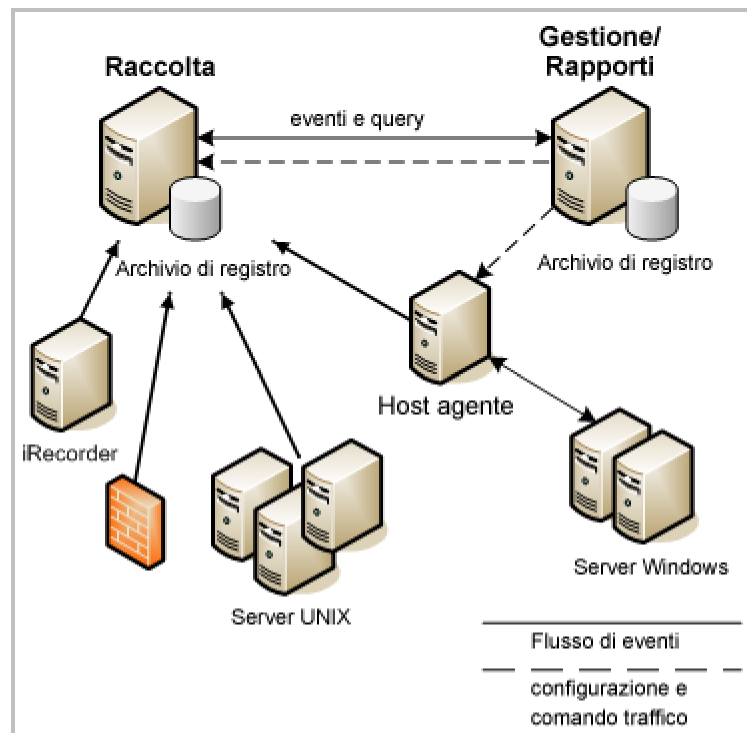
Nozioni fondamentali sull'ambiente CA Enterprise Log Manager

CA Enterprise Log Manager è realizzato per essere operativo poco tempo dopo l'inizio dell'installazione ed essere subito in grado di raccogliere informazioni sui registri e generare rapporti. È necessario installare l'applicazione software CA Enterprise Log Manager su un sistema dedicato.

Importante: poiché il server CA Enterprise Log Manager è dedicato alla raccolta dei registri eventi ad alte prestazioni, non installare altre applicazioni sul server che lo ospita. Altrimenti, ciò potrebbe avere ripercussioni negative sulle prestazioni.

Esistono numerosi approcci che è possibile utilizzare per configurare l'ambiente. Si consiglia la seguente configurazione specifica per meglio garantire la gestione di grandi quantità di eventi in ambienti aziendali.

Per un ambiente di produzione a livello aziendale di base, installare almeno due server CA Enterprise Log Manager nella rete esistente. I server CA Enterprise Log Manager utilizzano i server DNS esistenti all'interno della rete per operare con origini evento e agenti host indicati. Un server si occupa della raccolta e l'altro dei rapporti dei registri eventi raccolti. In un ambiente costituito da due server, il server di gestione che si installa per primo assume il ruolo di server di rapporto. In qualità di server di gestione, esegue l'autenticazione e l'autorizzazione degli utenti e svolge altre funzioni di gestione. La seguente illustrazione mostra questo ambiente di base con alcune origini evento:



Le righe continue in questo diagramma mostrano il flusso degli eventi dalle origini evento al server di raccolta o a un host agente e poi al server di raccolta. È possibile raccogliere direttamente eventi syslog utilizzando l'agente predefinito sul server di raccolta CA Enterprise Log Manager. È anche possibile configurare uno o più connettori su un host agente separato per eseguire la raccolta da diverse fonti syslog (non mostrate in questo diagramma).

La raccolta degli eventi di Windows utilizza Windows Management Instrumentation (WMI) per monitorare i server Windows per questi eventi. Ciò richiede la configurazione di un connettore WMI o di un agente installato su un host Windows come punto di raccolta di un evento. Per alcuni altri tipi di evento, si può decidere di utilizzare un CA iRecorder autonomo su un server host.

È possibile configurare e gestire gli agenti e i connettori di queste origini evento da qualsiasi server CA Enterprise Log Manager nella rete. Le linee tratteggiate nel diagramma rappresentano il traffico di configurazione e di controllo tra il server di gestione e gli agenti e ognuno degli altri server CA Enterprise Log Manager. Nell'ambiente raffigurato in questo diagramma, si eseguono le configurazioni dal server di gestione. Questo consente al server di raccolta di concentrarsi sull'elaborazione degli eventi.

L'ambiente di raccolta dei registri in cui si installano i server CA Enterprise Log Manager presenta le seguenti caratteristiche:

- Il server di gestione CA Enterprise Log Manager gestisce l'autenticazione e le autorizzazioni degli utenti e le configurazioni di tutti i server, degli agenti e dei connettori CA Enterprise Log Manager all'interno della rete utilizzando il suo server locale CA EEM.

  A seconda delle dimensioni della rete e della relativa quantità di eventi, è possibile scegliere di installare più di un server di gestione e creare federazioni di server di raccolta per ciascuno. Oppure è possibile dedicare diversi server alla creazione di rapporti, laddove tutti i server di rapporto sono registrati con il server di gestione. In questo scenario, il flusso degli eventi passa dalle origini evento al server di raccolta configurato al server di rapporto configurato.

- Uno o più server di raccolta CA Enterprise Log Manager elaborano e archiviano gli eventi in ingresso.
- Gli eventi passano attraverso la rete di raccolta degli eventi da una serie di origini evento *dopo* che vengono configurati i connettori o gli adapter corrispondenti.

Ulteriori informazioni:

Pianificazione server (a pagina 22)

Creazione dei DVD di installazione

Il software CA Enterprise Log Manager è disponibile come immagini ISO scaricabili e compresse. Dopo avere scaricato il software, è necessario creare supporti DVD prima di poter effettuare l'installazione. Utilizzare questa procedura per scaricare le immagini ISO e creare i dischi di installazione.

Per creare i DVD di installazione

1. Accedere al server di download all'indirizzo http://ca.com/support da un computer connesso a Internet.
2. Fare clic sul collegamento Technical Support e selezionare il collegamento Download Center.
3. Scegliere CA Enterprise Log Manager nel campo Select a Product e scegliere la versione di interesse nel campo Select a Release.
4. Selezionare la casella di controllo Select all components e fare clic su Go.

   Apparirà la pagina Published Solutions Downloads.
5. Selezionare il pacchetto da scaricare.

   Viene visualizzata la pagina del documento delle soluzioni.
6. Scorrere in fondo alla pagina e selezionare il collegamento Download di fianco al nome del pacchetto.

   Il download del pacchetto avrà inizio.

   Nota: il download potrebbe richiedere alcuni minuti prima del completamento, a seconda della velocità della connessione.
7. Decomprimere le due immagini dell'installazione.
8. Creare due dischi di installazione separati masterizzando il sistema operativo e le immagini del disco ISO CA Enterprise Log Manager su supporti DVD-RW separati.

   I due dischi di installazione contengono tutti i componenti del sistema operativo e del prodotto, rispettivamente, per l'ambiente CA Enterprise Log Manager. È possibile decidere di utilizzare nel proprio ambiente altri componenti come registratori SAPI o iRecorder. Si tratta di download separati disponibili sul sito Web di supporto di CA.
9. Utilizzare i dischi di installazione appena creati per eseguire le installazioni.

Installazione si un server CA Enterprise Log Manager

Per l'installazione, effettuare le seguenti operazioni:

- Completamento del foglio di calcolo del server CA Enterprise Log Manager
- Installazione del server di gestione CA Enterprise Log Manager.

  Nota: se si utilizza l'archiviazione SAN, evitare di installare su un'unità SAN.

- Installazione di uno o più server di raccolta CA Enterprise Log Manager
- (Facoltativo) Consente di installare uno o più server di rapporto

  Nota: se non viene installato un server dedicato ai rapporti, è possibile utilizzare il server di gestione per il ruolo del server di rapporto.
- (Facoltativo) Installazione di un server di punto di ripristino
- Verifica dell'installazione
- Visualizzazione degli eventi di automonitoraggio

Importante: Configurare i dischi di archiviazione in un array RAID *prima* di iniziare l'installazione di CA Enterprise Log Manager. Configurare i primi due dischi come RAID 1 e impostare questo array come array di avvio. Configurare i dischi rimanenti come array RAID 5 singolo. Se non viene configurato un array RAID si potrebbe verificare la perdita dei dati.

Per la sicurezza generale del server CA Enterprise Log Manager stesso, durante l'installazione l'utilità Grand Unified Boot-loader (GRUB) è protetta da password.

Foglio di lavoro del server CA Enterprise Log Manager

Prima di installare un server CA Enterprise Log Manager, raccogliere le informazioni nella seguente tabella. Una volta completato il foglio di lavoro, è possibile utilizzarlo mentre si lavora nei prompt di installazione. È possibile stampare e completare una serie di fogli di lavoro separati per ogni server CA Enterprise Log Manager che si ha intenzione di installare.

Informazioni CA Enterprise Log Manager	Valore	Commenti
Disco SO		
Tipo tastiera	*valore appropriato*	Specificare il tipo di tastiera che si desidera utilizzare per l'impostazione della lingua. Il valore predefinito corrisponde alle impostazioni hardware della tastiera connessa al server.
Selezione fuso orario	*fuso orario desiderato*	Selezionare il fuso orario del server.
Password principale	*nuova password principale*	Creare e confermare una nuova password per il server.

Informazioni CA Enterprise Log Manager	Valore	Commenti
Disco applicazione		
Nuovo nome host	*nome host per il server CA Enterprise Log Manager corrente* Ad esempio: CA-ELM1	Specificare il nome host del server utilizzando soltanto i caratteri supportati per gli host. Gli standard industriali consigliano l'utilizzo dei caratteri A-Z (senza distinzione di maiuscole), 0-9 ed i trattini, dove il primo carattere corrisponde ad una lettera e l'ultimo ad un carattere alfanumerico. Non utilizzare caratteri di sottolineatura. **Nota:** non aggiungere un nome dominio al valore del nome host.
Selezione di una periferica	*device name*	Selezionare il nome della scheda di rete da utilizzare per le raccolte e le comunicazioni degli eventi di log. Premere la barra spaziatrice per inserire la configurazione della periferica.
Indirizzo IP, Subnet mask e Gateway predefinito	*valori IP rilevanti*	Inserire un indirizzo IP valido per il server. Inserire una subnet mask ed un gate predefinito da utilizzare con il server.
Nome dominio	*il nome del dominio*	Inserire il nome dominio completo del server, ad esempio mycompany.com. **Nota:** per abilitare la risoluzione del nome host nell'indirizzo IP è necessario registrare il nome del dominio sul server DNS di rete.

Informazioni CA Enterprise Log Manager	**Valore**	**Commenti**
Elenco di server DNS	*indirizzi IPv4 o IPv6 corrispondenti*	Immettere uno o più indirizzi IP di server DNS utilizzati nella rete. elenco separato da virgole *senza* spazi tra le voci. Se i server DNS utilizzano indirizzi IPv6, immettere questi indirizzi in quel formato.
Data e ora di sistema	*data e ora locali*	Se necessario, inserire una nuova data e una nuova ora di sistema.
Aggiornare l'ora attraverso NTP?	Sì (consigliato) o No	Indicare se si vuole configurare il server CA Enterprise Log Manager per aggiornarne la data e l'ora da un server Network Time Protocol (NTP). **Nota:** la sincronizzazione dell'ora garantisce che gli avvisi contengano dati completi.
Nome o indirizzo del server NTP	*Nome host o indirizzo IP corrispondenti*	Immettere il nome host o l'indirizzo IP valido del server NTP da cui questo server CA Enterprise Log Manager riceve informazioni sulla data e l'ora.
EULA Sun Java JDK	Sì	Leggere il contratto di licenza facendo scorrere la pagina fino a visualizzare la domanda Accettare i termini della licenza sopracitati? [sì o no].
EULA CA	Sì	Leggere il contratto di licenza facendo scorrere la pagina fino a visualizzare la domanda Accettare i termini della licenza sopracitati? [sì o no].

Informazioni CA Enterprise Log Manager	Valore	Commenti
Server CA Embedded Entitlements Manager locale o remoto?	Locale: per il primo server installato (server di gestione) Remoto: per ogni server aggiuntivo	Indicare se si desidera utilizzare un server CA EEM locale o remoto. Per un server di gestione CA Enterprise Log Manager, scegliere il server remoto. L'installazione richiede di creare una password per l'account utente EiamAdmin predefinito. Per ogni server aggiuntivo, scegliere Remoto. L'installazione richiede il nome del server di gestione. Indipendentemente dal tipo di server scelto (locale o remoto), è necessario utilizzare l'ID e la password dell'account EiamAdmin per accedere per la prima volta a *ciascun* server CA Enterprise Log Manager.
Immettere il nome del server CA EEM	*Nome host o indirizzo IP*	Questo prompt viene visualizzato solo se si seleziona Remoto per il prompt del server locale o remoto. Immettere l'indirizzo IP o il nome host del server di gestione CA Enterprise Log Manager installato per primo. Il nome host deve essere registrato con il server DNS.

Informazioni CA Enterprise Log Manager	**Valore**	**Commenti**
Password amministratore del server CA EEM	*Password account EiamAdmin*	Registrare la password per l'account amministratore predefinito, EiamAdmin. L'accesso iniziale al server CA Enterprise Log Manager *richiede* queste credenziali dell'account. Se si installa il server di gestione, creare e confermare qui la nuova password EiamAdmin. Annotare questa password poiché essa verrà utilizzata nuovamente durante l'installazione degli altri server e agenti CA Enterprise Log Manager. **Nota:** la password qui inserita è anche la password iniziale dell'account caelmadmin predefinito che verrà utilizzato per accedere direttamente al server CA Enterprise Log Manager attraverso ssh. È possibile creare account amministratore aggiuntivi per accedere alle funzioni CA EEM dopo l'installazione, se lo si desidera.

Informazioni CA Enterprise Log Manager	Valore	Commenti
Nome istanza dell'applicazione	CAELM	Quando si installa il primo server CA Enterprise Log Manager della rete, si crea in questo prompt un valore istanza dell'applicazione. I server CA Enterprise Log Manager successivi utilizzano il valore per la registrazione con il server di gestione. Il nome istanza dell'applicazione predefinito è CAELM. È possibile utilizzare qualsiasi nome per il valore. Annotare il nome istanza dell'applicazione per le successive installazioni di CA Enterprise Log Manager.
Eseguire il server CAELM in modalità FIPS?	sì o no	La risposta al prompt determina se il server CA Enterprise Log Manager verrà avviato in modalità FIPS. **Nota:** se si aggiunge un server ad una distribuzione CA Enterprise Log Manager esistente, anche il server di gestione CA Enterprise Log Manager o il server remoto CA EEM dovranno essere in modalità FIPS. Se la modalità FIPS non viene abilitata, il nuovo server non potrà essere registrato e sarà necessario reinstallarlo.

Nota: l'installazione consente di verificare e modificare i dettagli relativi al server CA EEM prima che venga stabilita la connessione.

Se il programma di installazione non è in grado di connettersi al server di gestione specificato e si decide di continuare l'installazione, è possibile registrare il server CA Enterprise Log Manager manualmente con la funzionalità CA EEM incorporata. Se ciò accade, è necessario importare manualmente anche i file di gestione del contenuto, CEG e dell'agente. Fare riferimento alla sezione sulla risoluzione dei problemi legati all'installazione per ulteriori informazioni e istruzioni.

Ulteriori informazioni:

Registrare il server CA Enterprise Log Manager con il server CA EEM (a pagina 130)
Acquisizione di certificati dal server CA EEM (a pagina 131)
Importazione dei rapporti CA Enterprise Log Manager (a pagina 131)
Importazione dei file di mapping dei dati CA Enterprise Log Manager (a pagina 132)
Importazione dei file di analisi dei messaggi CA Enterprise Log Manager (a pagina 133)
Importazione dei file della grammatica evento comune (CEG) (a pagina 133)
Importazione dei file di gestione degli agenti comuni (a pagina 134)

Installazione di CA Enterprise Log Manager

Utilizzare questa procedura per installare un server CA Enterprise Log Manager.

Per installare il software CA Enterprise Log Manager

1. Avviare il server con il DVD di installazione del sistema operativo.

   L'installazione del sistema operativo si avvia automaticamente.

2. Rispondere ai prompt usando le informazioni raccolte nel foglio di calcolo del server CA Enterprise Log Manager.

   Rifiutando il Contratto di licenza, si interrompe l'installazione e il server viene arrestato.

3. Rispondere al prompt al riavvio rimuovendo prima il supporto e poi selezionando Riavvia.

4. Inserire il disco dell'applicazione CA Enterprise Log Manager quando richiesto e premere Invio.

5. Rispondere ai prompt usando le informazioni raccolte nel foglio di lavoro.

   Il processo di installazione prosegue. Quando viene visualizzato il messaggio "Installazione di CA Enterprise Log Manager riuscita", l'installazione è completa.

   Nota: quando si installa un secondo o successivo server CA Enterprise Log Manager, è possibile notare un messaggio di errore nel registro di installazione che indica che il nome dell'applicazione che l'installazione ha provato a registrare con il server CA EEM esiste già. È possibile ignorare in sicurezza questo errore, poiché ogni installazione di CA Enterprise Log Manager prova a creare il nome dell'applicazione come se fosse nuovo.

Al termine dell'installazione, è necessario configurare il server CA Enterprise Log Manager prima di potere ricevere eventi. Ciò può includere la configurazione di un connettore sull'agente predefinito per ricevere eventi syslog.

Ulteriori informazioni

Risoluzione di problemi dell'installazione (a pagina 128)
Configurazione dell'agente predefinito (a pagina 203)

Verifica dell'esecuzione del processo iGateway

Se non è possibile accedere all'interfaccia web del server CA Enterprise Log Manager dopo l'installazione e si è certi che le porte dell'interfaccia di rete siano configurate correttamente, probabilmente il processo igateway non è in esecuzione.

È possibile eseguire un controllo rapido dello stato del processo iGateway utilizzando questa procedura. Il processo iGateway deve essere in esecuzione affinché il server CA Enterprise Log Manager raccolga eventi e l'interfaccia utente sia accessibile.

Per verificare il daemon iGateway

1. Accedere ad un prompt dei comandi su un server CA Enterprise Log Manager.
2. Accedere con le credenziali dell'account caelmadmin.
3. Passare all'account dell'utente principale con il seguente comando:

   ```
   su - root
   ```

4. Utilizzare il seguente comando per verificare che il processo iGateway sia in esecuzione:

   ```
   ps -ef | grep igateway
   ```

   Il sistema operativo restituisce le informazioni sul processo iGateway e un elenco di processi in esecuzione in iGateway.

Ulteriori informazioni:

Risoluzione di errori di configurazione dell'interfaccia di rete (a pagina 129)

Avviare il daemon o il servizio iGateway

Il daemon o servizio iGateway è il processo che gestisce tutte le chiamate all'interfaccia utente sia per CA EEM che CA Enterprise Log Manager. Il processo deve essere in esecuzione per poter accedere ad entrambe le applicazioni. Utilizzare questa procedura per avviare il processo iGateway se non è in esecuzione.

Nota: se non si è in grado di avviare iGateway, assicurarsi che la cartella "/" disponga di spazio su disco. La mancanza di spazio su disco potrebbe impedire di avviare correttamente iGateway.

Per avviare il daemon o il servizio iGateway

1. Accedere come utente caelmadmin per il server CA Enterprise Log Manager.
2. Passare all'account dell'utente principale con il seguente comando:

   ```
   su -
   ```

3. Avviare il processo igateway con il seguente comando:

   ```
   $IGW_LOC/S99igateway start
   ```

   S99igateway è lo script di avvio del procsso igateway ed è di proprietà dell'utente principale. Quando viene avviato il processo igateway, viene eseguito con l'account utente caelmservice.

Terminare il daemon o il servizio iGateway

Il daemon o servizio iGateway è il processo che gestisce tutte le chiamate all'interfaccia utente sia per CA EEM che CA Enterprise Log Manager. Il processo deve essere in esecuzione per poter accedere ad entrambe le applicazioni. Utilizzare questa procedura per terminare il processo iGateway. Si potrebbe effettuare questa operazione in preparazione del riavvio del processo o rimuovendo un server CA Enterprise Log Manager dalla rete.

Per terminare il daemon o il servizio iGateway

1. Accedere come utente caelmadmin per il server CA Enterprise Log Manager.
2. Passare all'account dell'utente principale con il seguente comando:

   ```
   su -
   ```

3. Terminare il processo igateway con il seguente comando:

   ```
   $IGW_LOC/S99igateway stop
   ```

   S99igateway è lo script di avvio del processo igateway ed è di proprietà dell'utente principale. Quando viene avviato il processo igateway, viene eseguito con l'account utente caelmservice.

Avviare il daemon o il servizio dell'agente CA Enterprise Log Manager

Il daemon o il servizio dell'agente CA Enterprise Log Manager è il processo che gestisce i connettori che inviano gli eventi raccolti a un server CA Enterprise Log Manager. Il processo deve essere in esecuzione affinché i connettori possano raccogliere gli eventi. Utilizzare questa procedura per avviare il processo dell'agente CA Enterprise Log Manager se non è in esecuzione.

Per avviare il daemon o il servizio dell'agente CA ELM

1. Accedere come utente principale o amministratore Windows.
2. Accedere a un prompt dei comandi, quindi immettere il seguente comando:

   ```
   Linux, UNIX, Solaris:  /opt/CA/ELMAgent/bin/S99elmagent start
   ```

   ```
   Windows:  net start ca-elmagent
   ```

Terminare il daemon o il servizio dell'agente CA Enterprise Log Manager

Il daemon o il servizio dell'agente CA Enterprise Log Manager è il processo che gestisce i connettori che inviano gli eventi raccolti a un server CA Enterprise Log Manager. Il processo deve essere in esecuzione affinché i connettori possano raccogliere gli eventi. Utilizzare questa procedura per terminare il processo CA Enterprise Log Manager. Normalmente, i comandi di avvio e interruzione sono eseguiti dall'interno dell'Explorer agente su ogni server CA Enterprise Log Manager. È possibile utilizzare questo comando in preparazione del riavvio di un processo dell'agente e di tutti i suoi connettori.

Per terminare il daemon o il servizio dell'agente CA ELM

1. Accedere come utente principale o amministratore Windows.
2. Accedere a un prompt dei comandi, quindi immettere il seguente comando:

   ```
   Linux, UNIX, Solaris:  /opt/CA/ELMAgent/bin/S99elmagent stop
   ```

   ```
   Windows:  net stop ca-elmagent
   ```

Verifica dell'installazione del server CA Enterprise Log Manager

È possibile verificare l'installazione del server CA Enterprise Log Manager utilizzando un browser Web. È possibile eseguire una verifica iniziale dell'installazione effettuando l'accesso al server CA Enterprise Log Manager.

Nota: quando si accede all'applicazione CA Enterprise Log Manager per la prima volta, è necessario utilizzare le credenziali dell'utente EiamAdmin con cui è stato installato il server CA Enterprise Log Manager. Dopo avere effettuato l'accesso con questo account utente, è possibile vedere e utilizzare solo specifiche funzioni di gestione degli utenti e degli accessi. Si procede quindi con la configurazione dell'archivio utente e la creazione di un nuovo account utente CA Enterprise Log Manager per accedere ad altre funzionalità CA Enterprise Log Manager.

Per verificare il server CA Enterprise Log Manager

1. Aprire un browser Web e immettere il seguente URL:

   `https://<indirizzo_IP_server>:5250/spin/calm`

   Viene visualizzata la schermata di accesso a CA Enterprise Log Manager.

2. Effettuare l'accesso come utente amministrativo EiamAdmin.

   Apparirà la sottoscheda Gestione utenti e accessi della scheda Amministrazione. L'installazione è andata a buon fine se è possibile effettuare l'accesso al server CA Enterprise Log Manager.

   Nota: è necessario configurare uno o più servizi delle origini evento prima di potere ricevere i dati degli eventi e visualizzare i rapporti.

Visualizzazione degli eventi di automonitoraggio

È possibile utilizzare gli eventi di automonitoraggio per verificare che il server CA Enterprise Log Manager sia installato correttamente. Mentre sono presenti alcune attività di configurazione da completare prima che CA Enterprise Log Manager possa raccogliere e inviare rapporti sui dati dei registri eventi da qualsiasi punto della rete, è possibile vedere gli eventi di automonitoraggio generati immediatamente dal server CA Enterprise Log Manager.

L'accesso al server CA Enterprise Log Manager è la prima prova, e la migliore, di un'installazione eseguita correttamente. Gli eventi di automonitoraggio sono un altro modo per verificare lo stato del server CA Enterprise Log Manager. Sono disponibili diversi tipi di eventi di automonitoraggio. Utilizzare questa procedura per vedere dati aggiuntivi dagli eventi generati dal server CA Enterprise Log Manager stesso.

Per visualizzare eventi di automonitoraggio

1. Accedere al server CA Enterprise Log Manager.
2. Selezionare la scheda Rapporti.
3. Fare clic sulla scheda Sistema e selezionare il rapporto Dettagli eventi di automonitoraggio.

   Verrà caricato il rapporto sull'evento di automonitoraggio.

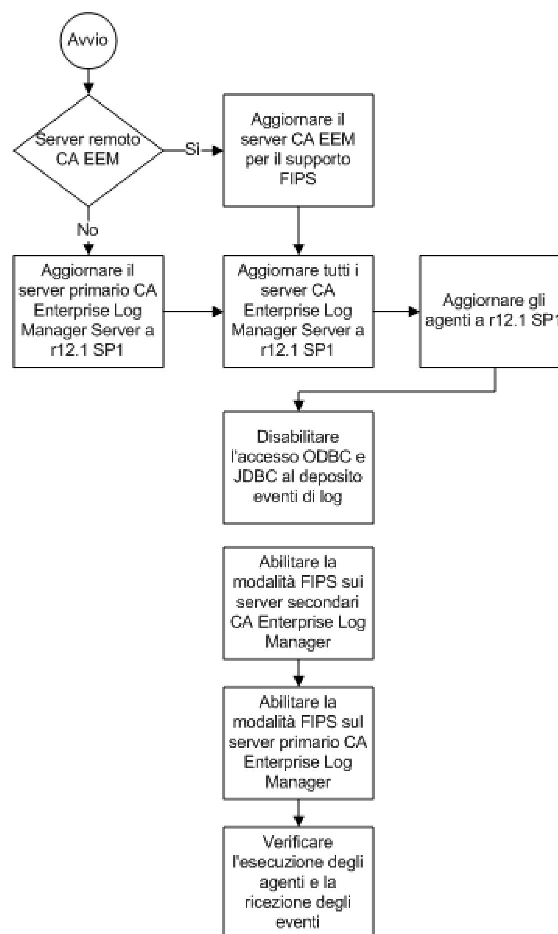
4. Verificare che gli eventi di automonitoraggio per l'accesso effettuato e altre azioni di configurazione preliminari siano presenti nel rapporto.

Aggiornamento di server e agenti CA Enterprise Log Manager esistenti per il supporto FIPS

È possibile eseguire l'aggiornamento di server e agenti CA Enterprise Log Manager per supporto FIPS mediante il modulo di sottoscrizione. Il processo di aggiornamento presuppone che:

- CA Enterprise Log Manager r12.1 sia installato o aggiornato a tale versione dalla versione r12.0 SP3.
- L'utente desidera attivare la modalità FIPS per la federazione CA Enterprise Log Manager.

Per aggiornare i server, procedere come segue:



Il processo di aggiornamento ed attivazione di FIPS include i seguenti passaggi:

1. Aggiornare il server primario o il server di gestione alla versione r12.1 SP1 o successive.

   Se si utilizza un server CA EEM remoto, assicurarsi che si trovi a un livello di versione che supporta FIPS. Consultare le *Note di rilascio di CA EEM* per ulteriori informazioni sull'aggiornamento del supporto FIPS.

   Istruzioni dettagliate per l'utilizzo del modulo di sottoscrizione per l'aggiornamento di server e agenti CA Enterprise Log Manager sono disponibili nella sezione relativa alla sottoscrizione della *Guida all'amministrazione*.

2. Aggiornare tutti gli altri server CA Enterprise Log Manager presenti nella federazione alla versione r12.1 SP1 o successive.

3. Aggiornare tutti gli agenti alla versione r12.1 SP1 o successive e i sensori log del connettore come richiesto.

   Importante: Se viene distribuito un connettore che utilizza il sensore di log syslog su un host Windows, aggiornare tutte le configurazioni del connettore per utilizzare la versione più recente del sensore syslog per questa versione, quando è in esecuzione in modalità FIPS. Fare riferimento alla Matrice di integrazione del prodotto https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/8238/8238_integration_certmatrix.html CA Enterprise Log Manager per l'elenco aggiornato delle integrazioni che utilizzano il sensore di log syslog.

4. Disabilitare l'accesso di ODBC e di JDBC al deposito eventi di log.

5. Attivare la modalità FIPS su ogni server secondario CA Enterprise Log Manager nella federazione.

   Gli agenti rilevano automaticamente la modalità dal server CA Enterprise Log Manager che li gestisce.

6. Attivare la modalità FIPS sul server primario o di gestione.

7. Verificare che gli agenti siano in esecuzione in modalità FIPS mediante il dashboard Gestione agenti.

   È inoltre possibile verificare che gli agenti inviino eventi utilizzando una query o un rapporto o controllando la scheda degli eventi di automonitoraggio nel servizio di stato del sistema.

Quando si esegue l'aggiornamento di un agente esistente alla versione r12.1 SP1 o a versioni successive, l'elaborazione della sottoscrizione aggiorna l'agente in modalità non FIPS per impostazione predefinita. È stata impostata la modalità FIPS per il server CA Enterprise Log Manager che gestisce un agente. Un agente rileva la modalità FIPS del server di gestione e riavvia se stesso nella modalità richiesta. Se si dispone di privilegi di amministratore, utilizzare il dashboard Gestione agenti nell'interfaccia utente di CA Enterprise Log Manager per visualizzare la modalità FIPS per un agente. Visualizzare le informazioni sugli aggiornamenti nella sezione relativa all'installazione CA Enterprise Log Manager della *Guida all'implementazione*, o consultare la Guida in linea per ulteriori informazioni su attività di gestione degli agenti.

Ulteriori informazioni:

Abilitare operazioni di modalità FIPS (a pagina 96)
Visualizzare il dashboard di agente (a pagina 97)

Prerequisiti per l'aggiornamento del supporto FIPS

Di seguito vengono riportati i prerequisiti per l'aggiornamento di CA Enterprise Log Manager al supporto FIPS 140-2:

- Avere installato CA Enterprise Log Manager r12.0 SP3 o r12.1
- Eseguire l'aggiornamento a CA Enterprise Log Manager r12.1 SP1 o versioni successive mediante sottoscrizione

Ulteriori informazioni:

Aggiunta di nuovi server CA Enterprise Log Manager in una federazione in modalità FIPS esistente (a pagina 99)

Linee guida sull'aggiornamento

Le seguenti linee guida sono valide per l'aggiornamento a CA Enterprise Log Manager con supporto FIPS:

- Se in una federazione sono presenti più server CA Enterprise Log Manager, aggiornare prima il server primario o il server di gestione CA Enterprise Log Manager alla versione r12.1 SP1 o successive. Quindi è possibile aggiornare tutti gli altri server in qualsiasi ordine. Il server viene avviato solo in modalità non FIPS. L'abilitazione della modalità FIPS richiede un utente con diritti di amministratore (per potere impostare la modalità manualmente).

  Importante: Non passare alla modalità FIPS su qualsiasi server secondario CA Enterprise Log Manager durante l'elaborazione della sottoscrizione. Ciò potrebbe causare l'interruzione del processo di sottoscrizione.

- I server CA Enterprise Log Manager della versione r12.1 SP1 o successive sono in grado di comunicare con gli agenti della versione r12.1, ma il supporto FIPS a livello di agente non è disponibile prima di eseguire l'aggiornamento.

- Quando viene attivata la modalità FIPS, solo gli agenti abilitati per FIPS nella versione r12.1 SP1 o successive possono comunicare con il server CA Enterprise Log Manager. Quando viene attivata la modalità *non* FIPS, il server CA Enterprise Log Manager è completamente compatibile con gli agenti di versioni precedenti, ma la modalità FIPS non è disponibile. È consigliabile installare *solo* agenti della versione r12.1 SP1 o successive dopo l'aggiornamento dei server CA Enterprise Log Manager alla versione r12.1 SP1 o successive.

- Gli agenti abilitati per FIPS associati a un server CA Enterprise Log Manager rilevano automaticamente le modifiche alla modalità del server e si riavviano nella modalità corrispondente.

- L'aggiunta di un nuovo server CA Enterprise Log Manager in una federazione esistente in esecuzione in modalità FIPS richiede una gestione speciale. Per ulteriori informazioni, consultare la sezione relativa all'aggiunta di un nuovo server CA Enterprise Log Manager in una federazione esistente della *Guida all'implementazione*.

- Se CA Enterprise Log Manager r12.1 SP1 è stato installato in modalità Non FIPS e si desidera eseguire l'aggiornamento a CA Enterprise Log Manager r12.1 in modalità FIPS, eseguire *una* delle operazioni seguenti:
    - Abilitare la modalità FIPS in CA Enterprise Log Manager r12.1 SP1 ed eseguire l'aggiornamento a CA Enterprise Log Manager r12.1 SP2 in modalità FIPS.
    - Eseguire l'aggiornamento a CA Enterprise Log Manager r12.1 SP2 in modalità non FIPS e abilitare la modalità FIPS in CA Enterprise Log Manager r12.1 SP2.

Ulteriori informazioni:

Abilitare operazioni di modalità FIPS (a pagina 96)

Aggiornamento di un server CA EEM remoto

Se si sta utilizzando un server CA EEM standalone con l'installazione di CA Enterprise Log Manager, aggiornare il server per il supporto FIPS prima di eseguire l'aggiornamento di qualsiasi altro server o agente di CA Enterprise Log Manager. Per ulteriori dettagli ed istruzioni, consultare la *Guida introduttiva di CA EEM*.

Disabilitare l'accesso ODBC e JDBC al deposito eventi di log

È possibile impedire l'accesso di ODBC e JDBC agli eventi nel deposito eventi di log utilizzando le opzioni della finestra di configurazione del servizio ODBC. Se si desidera eseguire una rete federata in modalità FIPS, disattivare l'accesso ODBC e JDBC per rimanere in conformità con gli standard della federazione.

Per disattivare l'accesso ODBC e JDBC

1. Accedere al server CA Enterprise Log Manager ed accedere alla scheda Amministrazione.
2. Fare clic sulla sottoscheda Servizi e quindi espandere il nodo Servizio ODBC.
3. Selezionare il server desiderato.
4. Deselezionare la casella di controllo Abilita servizio e fare clic su Salva.

   Nota: disabilitare l'opzione ODBC per *tutti* i server CA Enterprise Log Manager in una federazione per verificare che ODBC e JDBC siano disattivati.

Abilitare operazioni di modalità FIPS

Abilitare o disabilitare la modalità FIPS mediante le opzioni della modalità FIPS del servizio Stato del sistema. La modalità FIPS predefinita è non FIPS. Gli amministratori devono impostare la modalità FIPS per ogni server CA Enterprise Log Manager di una federazione.

Importante: Non è possibile utilizzare modalità miste all'interno di una stessa federazione di server. Se viene eseguita una modalità diversa su un server qualsiasi di una federazione questo non potrà recuperare i dati relativi a query e rapporti, né rispondere a richieste dagli altri server.

Per passare dalla modalità FIPS a non FIPS

1. Accedere al server CA Enterprise Log Manager.
2. Accedere alla scheda Amministrazione, quindi fare clic sulla sottoscheda Servizi.
3. Espandere il nodo del servizio Stato del Sistema e selezionare il server CA Enterprise Log Manager desiderato.

   Viene visualizzata la finestra di dialogo per la configurazione del servizio Stato del sistema.
4. Abilitare o disabilitare la modalità FIPS desiderata dall'elenco a discesa a seconda delle proprie esigenze..
5. Fare clic su Salva.

   Il server CA Enterprise Log Manager viene riavviato nella modalità selezionata. È `possibile ripetere l'accesso per visualizzare la modalità FIPS dell'agente da Gestione agenti.
6. Verificare la modalità operativa del server CA Enterprise Log Manager nella finestra di dialogo del servizio Stato del sistema dopo il riavvio del server.

   È anche possibile utilizzare eventi di automonitoraggio per verificare il riavvio del server CA Enterprise Log Manager nella modalità desiderata. Cercare i seguenti eventi nella scheda Eventi di automonitoraggio nella finestra di dialogo Stato del sistema:

   ```
   Modalità FIPS del server abilitata correttamente
   Modalità FIPS del server disabilitata correttamente
   Impossibile abilitare la modalità FIPS del server
   Impossibile disabilitare la modalità FIPS del server
   ```

La disabilitazione della modalità FIPS per il server primario o di gestione blocca il processo di restituzione dei dati delle query e dei rapporti federati. Inoltre, non vengono eseguiti i rapporti pianificati. Questa condizione persiste finché tutti i server della federazione non vengono eseguiti nuovamente nella stessa modalità.

Nota: la disabilitazione di FIPS sul server remoto o di gestione CA EEM è un requisito necessario per aggiungere un nuovo server CA Enterprise Log Manager a una federazione di server in esecuzione in modalità FIPS.

Ulteriori informazioni:

Disabilitare l'accesso ODBC e JDBC al deposito eventi di log (a pagina 95)

Visualizzare il dashboard di agente

È possibile visualizzare il dashboard di agente per visualizzare lo stato degli agenti nell'ambiente. Il dashboard visualizza inoltre alcuni dettagli come la modalità FIPS corrente (FIPS o non FIPS), e i dettagli di utilizzo. Questi includono il caricamento eventi al secondo, l'uso percentuale della CPU e la data e l'ora dell'ultimo aggiornamento.

Per visualizzare il dashboard di agente

1. Fare clic sulla scheda Amministrazione, e quindi sulla sottoscheda Raccolta registri.

   Verrà visualizzato l'elenco cartella di Raccolta registri.

2. Selezionare la cartella Explorer agente.

   Nel riquadro dei dettagli vengono visualizzati i pulsanti di gestione agente.

3. Fare clic su Monitoraggio di stato e dashboard di agente:

   Verrà visualizzato il riquadro di ricerca agente, che mostra lo stato di tutti gli agenti disponibili per mezzo di un grafico informativo. Ad esempio:

   ```
   Totale: 10 In esecuzione: 8 In sospeso: 1 Terminati: 1 Non risponde: 0
   ```

4. (Facoltativo) Selezionare i criteri di ricerca degli agenti per restringere l'elenco degli agenti visualizzati. È possibile selezionare uno o più criteri fra i seguenti:

   - Gruppo di agenti: restituisce solo gli agenti assegnati al gruppo selezionato.
   - Piattaforma: restituisce solo gli agenti in esecuzione sulla piattaforma selezionata.
   - Stato: restituisce solo gli agenti con lo stato selezionato, ad esempio In esecuzione.
   - Modello nome agente: restituisce solo gli agenti contenenti il modello specificato.

5. Fare clic su Mostra stato.

   Verrà visualizzato un elenco degli agenti che soddisfano i criteri di ricerca, con l'aggiunta di una serie di informazioni fra cui:

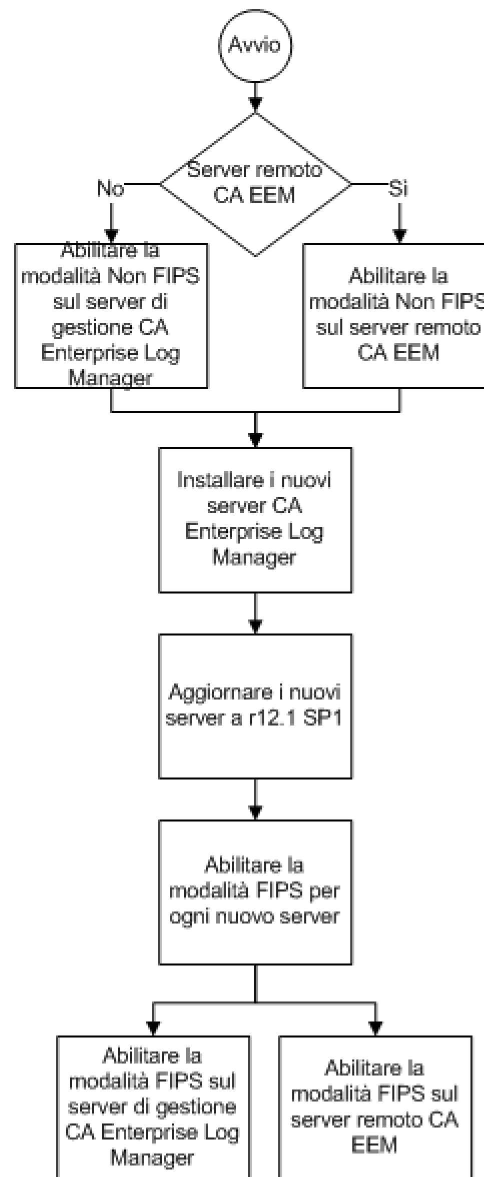
   - Nome e versione del connettore locale
   - Server CA Enterprise Log Manager corrente
   - Modalità FIPS dell'agente (FIPS o non FIPS)
   - Ultimo carico di eventi al secondo registrato e gestito dall'agente
   - Ultimo valore di utilizzo della CPU registrato
   - Ultimo valore di utilizzo della memoria registrato
   - Ultimo aggiornamento di configurazione
   - Stato dell'aggiornamento di configurazione

Aggiunta di nuovi server CA Enterprise Log Manager in una federazione in modalità FIPS esistente

Sono disponibili delle linee guida speciali per l'aggiunta di un nuovo server CA Enterprise Log Manager in una federazione di server già in esecuzione in modalità FIPS. Se la modalità FIPS non viene specificata durante l'installazione, i nuovi server CA Enterprise Log Manager installati verranno eseguiti in modalità *non* FIPS per impostazione predefinita. I server in esecuzione in modalità non FIPS non possono comunicare con i server in esecuzione in modalità FIPS.

Come parte dell'installazione, è necessario che un nuovo server CA Enterprise Log Manager venga registrato con il server locale CA EEM incorporato nel server di gestione, o con un server standalone remoto di CA EEM. I processi di aggiunta di un server a una rete esistente sono basati sul percorso del server di gestione CA EEM.

Considerare il seguente flusso di lavoro:



Il processo di aggiunta di un nuovo server comprende i seguenti passaggi:

1. Verificare che la modalità FIPS sia abilitata sul server di gestione (primario) CA Enterprise Log Manager o sul server remoto CA EEM.
2. Installare uno o più nuovi server secondari CA Enterprise Log Manager mediante l'immagine ISO o i DVD per CA Enterprise Log Manager 12.1 SP1 o versioni successive.

   Importante: Accertarsi di specificare la modalità FIPS durante l'installazione. In caso contrario, il nuovo server installato non potrà comunicare con il server di gestione o il server remoto CA EEM e sarà necessario reinstallare il nuovo server CA Enterprise Log Manager.

L'abilitazione della modalità FIPS per il server di gestione CA Enterprise Log Manager o per il server remoto CA EEM consente di registrare il nuovo server CA Enterprise Log Manager e di associarlo alla federazione.

Ulteriori informazioni:

Abilitare operazioni di modalità FIPS (a pagina 96)
Visualizzare il dashboard di agente (a pagina 97)

Considerazioni sull'installazione di sistemi con unità di SAN

Quando si installa il sistema operativo per l'applicazione CA Enterprise Log Manager su un sistema con unità SAN, procedere con cautela per evitare che CA Enterprise Log Manager venga installato su una unità SAN. Una installazione di questo tipo non verrà eseguita.

Selezionare uno dei seguenti approcci per garantire una corretta installazione:

- Disattivare le unità SAN. installare il sistema operativo e l'applicazione CA Enterprise Log Manager come di consueto. Quindi, configurare le unità SAN per CA Enterprise Log Manager e riavviare CA Enterprise Log Manager per attivare la configurazione SAN.
- Lasciare le unità SAN abilitate. Avviare l'installazione del sistema operativo. Uscire dalla procedura per modificare la sequenza di operazioni definite nel file di kickstart. Riprendere il processo di installazione e completarlo come descritto.

Installazione con unità SAN disabilitate

CA Enterprise Log Manager non è attualmente supportato tramite configurazioni hardware fisse fornite da Dell, IBM e HP. Il seguente esempio presuppone che l'hardware sia costituito da HP Blade Servers con una scheda QLogic Fibre Channel per la connessione a una SAN per l'archiviazione dei dati. HP Blade Servers è accompagnato dal disco rigido SATA configurato in RAID-1 (con mirroring).

Se si utilizza il file di avvio kickstart, disattivare le unità SAN prima di iniziare l'installazione. Avviare il processo di installazione con il DVD OS5 e completare l'installazione come documentato.

Nota: se l'installazione non viene avviata con l'unità SAN disabilitata, CA Enterprise Log Manager viene installato sulla SAN. In questo caso, viene visualizzata una schermata con il messaggio codice operativo non valido dopo il riavvio di CA Enterprise Log Manager.

utilizzare la seguente sequenza di procedure per installare un'applicazione CA Enterprise Log Manager su un sistema con unità SAN in cui viene disattivata l'unità SAN prima di installare il sistema operativo.

1. Disattivare le unità SAN.
2. Installare il sistema operativo sull'applicazione.
3. Installare il server CA Enterprise Log Manager.
4. Impostare una configurazione con più percorsi per l'archiviazione SAN.
5. Creare un volume logico.
6. Preparare il volume logico per CA Enterprise Log Manager.
7. Riavviare CA Enterprise Log Manager.
8. Verificare l'esito dell'installazione.

Durante l'installazione del sistema operativo con le unità SAN disabilitate, verranno utilizzati i seguenti file:

lvm.conf

File di configurazione per Linux Logical Volume Manager (LVM2).

multipath.conf (/etc/multipath.conf)

File di configurazione per più percorsi Linux.

fstab (/etc/fstab)

File di tabella del file system che esegue il mapping di dispositivi in directory di un sistema Linux.

Disattivazione delle unità SAN

Utilizzare le procedure consigliate dal fornitore dell'unità SAN per disattivare le unità SAN nel nuovo hardware su cui si desidera installare l'applicazione.

Disattivare le unità SAN prima di installare il sistema operativo dell'applicazione o l'applicazione CA Enterprise Log Manager.

Impostazione di una configurazione con più percorsi per l'archiviazione SAN

L'impostazione di una configurazione con più percorsi è richiesta per un sistema CA Enterprise Log Manager installato su un sistema RAID che utilizza l'archiviazione SAN. I dischi fisici sulla SAN sono partizionati in spazi di archiviazione logica denominati LUN (numeri di unità logica).

Impostazione di una configurazione con più percorsi per l'archiviazione SAN

1. Accedere all'applicazione CA Enterprise Log Manager e spostarsi alla directory principale.
2. (Facoltativo) Visualizzare un elenco delle directory di /dev/mapper per visualizzare lo stato della configurazione prima di impostare percorsi multipli e volumi logici. Verranno visualizzati dei risultati simili ai seguenti:

```
drwxr-xr-x  2 root root     120 Jun 18 12:09 .
drwxr-xr-x 11 root root    3540 Jun 18 16:09 ..
crw-------  1 root root  10, 63 Jun 18 12:09 control
brw-rw----  1 root disk 253,  0 Jun 18 16:09 VolGroup00-LogVol00
brw-rw----  1 root disk 253,  2 Jun 18 12:09 VolGroup00-LogVol01
brw-rw----  1 root disk 253,  1 Jun 18 16:09 VolGroup00-LogVol02
```

3. Aprire il file .../etc/multipath.conf per la modifica e procedere come indicato di seguito:

   a. Aggiungere la seguente sezione sotto "device {" per ogni LUN fornito dall'amministratore della SAN:

```
device {
    vendor                 "NETAPP"
    product                "LUN"
    path_grouping_policy   multibus
    features               "1 queue_if_no_path"
    path_checker           readsector0
    path_selector          "round-robin 0"
    failback               immediate
    no_path_retry          queue
         }
```

   b. Rimuovere il commento dalla sezione "blacklist" per tutti i dispositivi. La sezione blacklist abilita percorsi multipli su periferiche predefinite.

```
blacklist {
    devnode "^(ram|raw|loop|fd|md|dm-|sr|scd|st)[0-9]*"
    devnode "^hd[a-z]"
    devnode "^cciss!c[0-9]d[0-9]*"
}
```

   c. Salvare e chiudere il file multipath.conf.

4. Verificare che i percorsi siano attivi e che i LUN siano elencati per eseguire le seguenti operazioni:

```
multipath -l
```

   Nota: i percorsi vengono visualizzati come ‘mpath0’’ e ‘mpath1’. Se i LUN non vengono visualizzati, riavviare il computer e eseguire di nuovo i percorsi multipli.

5. Visualizzare le unità disponibili.

```
fdisk -l
```

6. Elencare le partizioni disponibili e verificare che 'mpath0' e 'mpath1' siano nell'elenco.

```
ls -la /dev/mapper
```

7. Mappare la prima partizione come segue:

```
kpartx -a /dev/mapper/mpath0
```

8. Mappare la seconda partizione come segue:

```
kpartx -a /dev/mapper/mpath1
```

Creazione di un volume logico

È possibile utilizzare il software di gestione dei volumi per combinare più LUN in un volume logico per l'accesso di CA Enterprise Log Manager. Logical Volume Manager (LVM) consente di gestire le unità disco e dispositivi di archiviazione di massa simili nel sistema operativo Linux. Le colonne di archiviazione creata in LVM possono essere ridimensionate o spostate in dispositivi backend come l'archiviazione SAN.

Per creare un volume logico

1. Creare il primo volume fisico:

   ```
   pvcreate /dev/mapper/mpath0
   ```

2. Creare il secondo volume fisico:

   ```
   pvcreate /dev/mapper/mpath1
   ```

3. Mostrare tutti i volumi fisici sul sistema:

   ```
   pvdisplay
   ```

4. Creare il gruppo volume VolGroup01 (il gruppo volume VolGroup00 esiste già).

   ```
   vgcreate VolGroup01 /dev/mapper/mpath0 /dev/mapper/mpath1
   ```

   Nota: questo comando crea un volume e rende i due volumi fisici parte del gruppo.

5. Creare un volume logico nel volume gruppo:

   ```
   lvcreate –n LogVol00 –l 384030 VolGroup01
   ```

6. Creare un file system:

   ```
   mkfs –t ext3 /dev/VolGroup01/LogVol00
   ```

Preparazione di un volume logico per CA Enterprise Log Manager

Dopo aver creato un volume logico, compilarlo con la struttura di directory prevista e assegnare la proprietà e le associazioni gruppo richieste da CA Enterprise Log Manager. Utilizzare vi per modificare il file fstab per puntare a un volume logico creato e quindi montare la nuova directory dei dati.

Per preparare il volume logico per CA Enterprise Log Manager

1. Creare una directory temporanea, /data1, modificare la proprietà della directory /data1 a caelmservice e modificare il gruppo associato a questa directory in caelmservice:

   ```
   mkdir /data1
   chown caelmservice /data1
   chgrp caelmservice /data1
   ```

2. Interrompere i processi iGateway del server CA Enterprise Log Manager:

   ```
   /opt/CA/SharedComponents/iTechnology/S99igateway stop
   ```

3. Spostarsi alla directory in cui l'agente di CA Enterprise Log Manager è in esecuzione, interrompere l'agente e verificare che i servizi non siano in esecuzione:

   ```
   cd /opt/CA/ELMAgent/bin/
   ./caelmagent –s
   ps –ef | grep /opt/CA
   ```

4. Passare alla directory / directory.

5. Montare il nuovo file system su /data1, copiare i contenuti della directory /data nella directory /data1, e verificare che le due directory siano uguali:

   ```
   mount –t ext3 /dev/VolGroup01/LogVol00 /data1
   cp –pR /data/* /data1
   diff –qr /data /data1
   ```

6. Smontare il punto di montaggio dei dati esistente e quindi smontare il punto di montaggio di data1:

   ```
   umount /data
   umount /data1
   ```

7. Eliminare la directory /data e rinominare la directory /data1 in /data.

   ```
   rm –rf /data
   mv /data1 data
   ```

8. Modificare la riga in /etc/fstab che fa riferimento alla directory /data e puntarla al nuovo volume logico. Quindi, modificare /dev/VolGroup00/LogVol02 in /dev/VolGroup01/LogVol00. I dati modificati vengono indicati in grassetto nel seguente rendering di un file fstab campione.

nome della periferica	punto di montaggio	fs-type	Opzioni	dump-freq pass-num
nessuno	/dev/VolGroup00/LogVol00/	ext3	valori predefiniti	1 1
nessuno	**/dev/VolGroup01/LogVol00/data**	ext3	valori predefiniti	1 2
LABEL=/boot	/boot	ext3	valori predefiniti	1 2
tmpfs	/dev/shm	tmpfs	valori predefiniti	0 0
devpts	/dev/pts	devpts	gid=5,mode=620	0 0
sysfs	/sys	sysfs	valori predefiniti	0 0
l'indirizzo	/proc	l'indirizzo	valori predefiniti	0 0
nessuno	/dev/VolGroup00/LogVol01	swap	valori predefiniti	0 0

9. Montare la nuova directory dei dati e verificare che tutte le partizioni in /etc/fstab siano montate:

```
mount -a
```

```
montaggio
```

Riavvio del server CA Enterprise Log Manager

Dopo aver creato un volume logico, riavviare CA Enterprise Log Manager in modo che sia possibile utilizzare il volume logico. Per verificare l'esito dell'operazione, passare a CA Enterprise Log Manager e visualizzare gli eventi restituiti dalla query Dettagli relativi a tutti gli eventi di sistema.

Per riavviare il server CA Enterprise Log Manager

1. Avviare i processi iGateway del server CA Enterprise Log Manager:

```
/opt/CA/SharedComponents/iTechnology/S99igateway start
```

2. Avviare il servizio ELMAgent.

```
/opt/CA/ELMAgent/bin/caelmagent –b
```

3. Riavviare il server CA Enterprise Log Manager.

Installazione con unità SAN abilitate

L'argomento Esempio: Impostazione dell'archiviazione SAN per CA Enterprise Log Manager include il suggerimento per disattivare le unità SAN (LUN) prima di installare il sistema operativo sull'applicazione CA Enterprise Log Manager.

Un'alternativa è lasciare le unità SAN abilitate modificando il file di kickstart, ca-elm-ks.cfg, con uno strumento di modifica ISO dopo l'avvio del sistema operativo. La modifica consente di verificare che l'installazione e l'avvio vengono eseguiti dal disco rigido locale, non dalla SAN.

Per avviare il sistema dal disco locale (SAN)

1. Avviare il server con il DVD di installazione del sistema operativo
2. Rispondere al primo prompt sul tipo di tastiera.
3. Premere Alt-F2 per visualizzare il prompt Anaconda/Kickstart.
4. Digitare la seguente stringa:

   ```
   list-hardrives
   ```

   Viene visualizzato l'elenco di unità disponibili, in cui l'elenco è simile a quello illustrato di seguito:

   ```
   cciss/c0d0 – 68GB RAID 1 (cciss è HP Smart Array)
   Sda – 500GB SAN  (sda – h è SAN Multipathed)
   Sdb – 500GB SAN
   Sdc – 500GB SAN
   Sdd – 500GB SAN
   Sde – 500GB SAN
   Sdf – 500GB SAN
   Sdg – 500GB SAN
   Sdh – 500GB SAN
   ```

5. Identificare il disco rigido locale. In questo caso, si tratta di cciss/c0d0.

6. Procedere come segue:

   a. Aprire il file di kickstart del sistema operativo di CA Enterprise Log Manager, ca-elm-ks.cfg, per la modifica. utilizzare un editor ISO.

   b. Individuare la seguente riga da modificare:

   ```
   bootloader --location=mbr --driveorder=sda,sdb
   ```

   Modificarla in:

   ```
   bootloader --location=mbr --driveorder=cciss/c0d0
   ```

   Questa modifica specifica l'avvio solo dal disco locale.

   c. Individuare le seguenti righe da modificare:

   ```
   clearpart --all --initlabel
   part /boot --fstype "ext3" --size=100
   part pv.4 --size=0 –grow
   ```

   Modificare queste righe come di seguito:

   ```
   part /boot --fstype "ext3" --size=100 --ondisk cciss/c0d0
   part pv.4 --size=0 --grow --ondisk cciss/c0d0
   ```

   Questa modifica alle righe di definizione delle partizioni consente di garantire che le partizioni vengano create per nome sul disco cciss/c0d0. Utilizzando --ondisk, vengono sostituite le variabili $disk1 e $disk2 esistenti.

   d. In caso fosse necessario, rimuovere la clausola IF/When per il numero di unità disco, mantenendo solo il primo insieme di comandi del disco (righe 57 - 65).

   e. Salvare la nuova immagine ISO.

7. uscire dal prompt Anaconda per tornare ai prompt di installazione del sistema operativo.

8. Continuare l'installazione utilizzando le procedure indicate.

Configurazioni server CA Enterprise Log Manager iniziali

L'installazione del primo server CA Enterprise Log Manager crea un nome applicazione il cui valore predefinito è CAELM. L'installazione registra questo nome con il server CA EEM incorporato. Quando installazioni successive utilizzano lo stesso nome dell'istanza dell'applicazione, il server di gestione CA Enterprise Log Manager gestisce tutte le configurazioni con lo stesso nome dell'istanza dell'applicazione.

Al termine dell'installazione, il server sarà dotato sia di un sistema operativo che di un server CA Enterprise Log Manager. Il sistema operativo a 32 bit supporta sia hardware a 32 che a 64 bit. Le configurazioni iniziali includono le seguenti aree:

- Account utente predefinito
- Struttura directory predefinita
- Immagine personalizzata del sistema operativo
- Assegnazioni delle porte predefinite

Account utente predefinito

L'installazione di CA Enterprise Log Manager crea un utente amministratore predefinito, caelmadmin, che dispone della propria password. Quando è necessario effettuare l'accesso diretto al server host, è necessario utilizzare questo account per accedere, perché la possibilità di accesso dell'account dell'utente principale viene limitata dopo l'installazione. L'account caelmadmin permette solo un'azione di accesso. Da questo punto è necessario commutare gli utenti all'account dell'utente principale utilizzando la sua password separata per accedere alle utilità di amministrazione a livello del SO.

La password predefinita per questo account è la stessa password creata per l'account EiamAdmin. Si consiglia di modificare la password dell'account caelmadmin subito dopo l'installazione.

L'installazione crea anche un account predefinito di utente di servizio, caelmservice, che *non* è possibile utilizzare per accedere al sistema. È possibile commutare gli utenti a questo utente per avviare e interrompere i processi, se necessario. Il processo iGateway e il server CA EEM incorporato (se è presente uno installato sul server CA Enterprise Log Manager) vengono eseguiti da questo account utente per fornire livelli aggiuntivi di sicurezza.

Il processo iGateway non viene eseguito nell'account dell'utente principale. L'inoltro delle porte viene abilitato automaticamente per consentire le richieste HTTPS sulle porte 80 e 443 per accedere all'interfaccia utente di CA Enterprise Log Manager, oltre alla porta 5250.

Struttura directory predefinita

L'installazione di CA Enterprise Log Manager posiziona file binari del software nella struttura della directory /opt/CA. Se il sistema ha una seconda unità disco, viene configurata come /data. L'installazione crea un collegamento simbolico dalla directory /opt/CA/LogManager/data alla directory /data. Quanto segue rappresenta la struttura della directory di installazione predefinita:

Tipi di file	Directory
File relativi ad iTechnology (iGateway)	/opt/CA/SharedComponents/iTechnology
File relativi al server CA Enterprise Log Manager EEM	/opt/CA/LogManager/EEM
File relativi all'installazione di CA Enterprise Log Manager	/opt/CA/LogManager/install
File di dati (collegamenti a /data in caso di unità diverse)	/opt/CA/LogManager/data
File registro	/opt/CA/SharedComponents/iTechnology

In circostanze normali, non è necessario accedere all'utilità *ssh* sul server CA Enterprise Log Manager, eccetto per spostare file di archivi per il backup e l'archiviazione a lungo termine e per aggiungere unità disco.

Immagine personalizzata del sistema operativo

Il processo di installazione personalizza il sistema operativo creando un'immagine minima e limitando l'accesso al minor numero di canali possibile. I servizi non essenziali non vengono installati. Il server CA Enterprise Log Manager è in ascolto su un numero ristretto di porte e chiude automaticamente le porte non utilizzate.

Durante l'installazione del sistema operativo, si crea una password per l'account dell'utente principale. Al termine dell'installazione di CA Enterprise Log Manager, l'utente principale è limitato in modo da non permettere login successivi. L'installazione di CA Enterprise Log Manager crea un utente predefinito, *caelmadmin*, che dispone solo di possibilità di accesso e di nessun'altra autorizzazione.

Per accesso a livello principale al server CA Enterprise Log Manager, è possibile accedere al server con questo account e passare all'account dell'utente principale per l'utilizzo degli strumenti di amministrazione. Ciò significa che si dovrà conoscere la password sia di *caelmadmin* che di *root* per avere accesso al sistema come utente principale.

Con CA Enterprise Log Manager non viene installato nessun altro software specifico relativo alla sicurezza. Per mantenere prestazioni elevate, non installare altre applicazioni sul server CA Enterprise Log Manager.

Assegnazioni delle porte predefinite

Il server CA Enterprise Log Manager è configurato per impostazione predefinita per l'ascolto sulla porta 5250 e sulle porte 80 e 443 utilizzando il protocollo HTTPS. Le procedure e i daemon CA Enterprise Log Manager non vengono eseguiti nell'account root, quindi non possono aprire porte inferiori alla porta 1024. Di conseguenza, l'installazione crea automaticamente un reindirizzamento (attraverso iptables) alla porta 5250 per le richieste dell'interfaccia utente sulle porte 80 e 443.

Il daemon syslog del sistema operativo locale del server CA Enterprise Log Manager non è configurato, poiché CA Enterprise Log Manager utilizza i propri eventi di automonitoraggio per tracciare lo stato del sistema. È possibile visualizzare altri eventi locali e rapporti sulle azioni intraprese sul server CA Enterprise Log Manager locale utilizzando eventi di automonitoraggio.

Di seguito si trova un elenco di porte utilizzate dall'ambiente CA Enterprise Log Manager:

Porta	Componente	Descrizione
53	Server CA Enterprise Log Manager	La porta TCP/UDP che deve essere disponibile per le comunicazioni DNS per risolvere i nomi host negli indirizzi IP dei server come i server CA Enterprise Log Manager, il server remoto CA EEM, se configurato, e il server NTP se è stata selezionata la sincronizzazione con l'ora NTP al momento dell'installazione. Le comunicazioni DNS non sono necessarie se i nomi host sono stati mappati negli indirizzi IP nel file /etc/hosts locale.
80	Server CA Enterprise Log Manager	Comunicazioni TCP con l'interfaccia utente del server CA Enterprise Log Manager attraverso HTTPS; ridirezionamento automatico alla porta 5250

Porta	Componente	Descrizione
111	Portmapper (SAPI)	Comunicazioni client di controllo con il processo PortMapper per ricevere assegnazioni delle porte dinamiche
443	Server CA Enterprise Log Manager	Comunicazioni TCP con l'interfaccia utente del server CA Enterprise Log Manager attraverso HTTPS; ridirezionamento automatico alla porta 5250
514	Syslog	Porta di ascolto UDP predefinita di syslog; il valore di questa porta può essere configurato Affinché l'agente predefinito venga eseguito come utente non di root, la porta predefinita è impostata su 40514 e l'installazione applica una regola di firewall al server CA Enterprise Log Manager.
1468	Syslog	Porta di ascolto TCP predefinita di syslog; il valore di questa porta può essere configurato
2123	DXadmin	Porta DXadmin LDAP di CA Directory, se viene utilizzato un server CA EEM sullo stesso server fisico del server CA Enterprise Log Manager (il server di gestione).
5250	Server CA Enterprise Log Manager	Comunicazioni TCP con l'interfaccia utente del server CA Enterprise Log Manager utilizzando iGateway Comunicazioni TCP tra: ■ Server CA Enterprise Log Manager e server CA EEM ■ Server CA Enterprise Log Manager federati ■ Agente e server CA Enterprise Log Manager per aggiornamenti dello stato
6789	Agente	Porta di ascolto di comando e controllo dell'agente **Nota:** se non si consente il traffico in uscita, sarà necessario aprire questa porta per consentire il funzionamento corretto.
17001	Agente	Porta TPC per comunicazioni sicure tra agente e server CA Enterprise Log Manager; il valore di questa porta può essere configurato **Nota:** se non si consente il traffico in uscita, sarà necessario aprire questa porta per consentire il funzionamento corretto.
17002	ODBC/JDBC	Porta TCP predefinita utilizzata per le comunicazioni tra i driver ODBC o JDBC e il deposito eventi di log di CA Enterprise Log Manager.

Porta	Componente	Descrizione
17003	Agente	Porta TCP usata per le comunicazioni dal bus messaggi Qpid per gli agenti r12.1.
57000	Dispatcher listener SME	Porta TCP usata per il servizio Dispatcher sull'host locale dell'agente per l'ascolto degli eventi di automonitoraggio tra i processi dell'agente.
57001	Dispatcher listener eventi	Porta TCP utilizzata per il servizio Dispatcher è abilitata per SSL (usando ETPKI) per l'ascolto di eventi dai connettori client.
casuale	SAPI	Porte UDP per la raccolta eventi assegnate dalla mappatura delle porte; è possibile configurare il router e il collector SAPI per utilizzare qualsiasi valore di porta fisso superiore a 1024

Elenco dei processi correlati

La seguente tabella rappresenta un elenco dei processi eseguiti come parte di un'implementazione CA Enterprise Log Manager. L'elenco non include processi di sistema relativi al sistema operativo sottostante.

Process Name	Porta predefinita	Descrizione
caelmagent	6789, 17001	Questo è il processo dell'agente CA Enterprise Log Manager.
caelmconnector	Dipende da ciò che ascolta o a cui si connette.	Questo è il processo del connettore CA Enterprise Log Manager. Sarà presente un altro processo del connettore separato in esecuzione per ogni connettore configurato su un agente.
caelmdispatcher		Questo processo CA Enterprise Log Manager gestisce l'invio di eventi e le informazioni sullo stato tra il connettore e l'agente.
caelmwatchdog	Nessuno	Il processo di controllo di CA Enterprise Log Manager che esegue il monitoraggio di altri processi per garantire la continuità delle operazioni.
caelm-agentmanager		Questo processo di CA Enterprise Log Manager gestisce le attività di gestione dell'agente quali lo stato e la sottoscrizione.

Process Name	Porta predefinita	Descrizione
caelm-alerting		Questo processo di CA Enterprise Log Manager gestisce i messaggi di avviso inviati mediante posta elettronica, IT PAM e trap SNMP.
caelm-correlation		Questo processo di CA Enterprise Log Manager gestisce le regole di correlazione mediante la comunicazione con il servizio di correlazione in caso di attivazione delle regole di correlazione.
caelm-eemsessionsponsor		Il processo principale di CA EEM che gestisce tutte le comunicazioni verso CA EEM per gli sponsor locali in esecuzione in safetynet sul server CA Enterprise Log Manager. Questo processo può essere eseguito in safetynet.
caelm-incidentservice		Questo processo di CA Enterprise Log Manager gestisce la generazione degli incidenti e la configurazione della registrazione mediante la gestione delle informazioni provenienti dal servizio di correlazione in caso di attivazione di una regola di correlazione.
caelm-logdepot	17001	Il processo di archiviazione del log eventi CA Enterprise Log Manager che gestisce l'archiviazione di eventi, la creazione di file di archiviazione e altre funzioni. Questo processo può essere eseguito in safetynet.
caelm-queryservice		Questo processo di CA Enterprise Log Manager viene utilizzato per la configurazione e la gestione delle query.
caelm-reporter		Questo processo di CA Enterprise Log Manager viene utilizzato per la configurazione e la gestione dei rapporti pianificati, delle esportazioni dei rapporti e degli avvisi.
caelm-ruletest		Questo processo di CA Enterprise Log Manager gestisce i test della regola eseguiti ad hoc.
caelm-sapicollector		Il processo del servizio Collector SAPI. Questo processo può essere eseguito in safetynet.

Process Name	Porta predefinita	Descrizione
caelm-sapirouter		Il processo del servizio router SAPI. Questo processo può essere eseguito in safetynet.
caelm-systemstatus		Questo processo raccoglie lo stato del sistema per la visualizzazione nell'interfaccia utente CA Enterprise Log Manager. Questo processo può essere eseguito in safetynet.
dxadmind		Processo di CA Directory eseguito su un server su cui è installato CA EEM.
dxserver		Processo di CA Directory eseguito su un server su cui è installato CA EEM.
igateway	5250	Processo principale CA Enterprise Log Manager; deve essere in esecuzione per raccogliere e archiviare eventi.
broker messaggi		Processo di CA Enterprise Log Manager che comunica tra l'agente e il server CA Enterprise Log Manager per l'invio di eventi.
oaserver	17002	Processo di CA Enterprise Log Manager eseguito per gestire l'elaborazione lato server delle richieste ODBC e JDBC per l'accesso all'archivio del log eventi.
safetynet		Framework del processo CA Enterprise Log Manager eseguito per garantire la continuità delle operazioni.
ssld		Processo di CA Directory eseguito su un server su cui è installato CA EEM.

Protezione avanzata del sistema operativo

il dispositivo software CA Enterprise Log Manager contiene una copia semplice e avanzata del sistema operativo Red Hat Linux. Le seguenti tecniche di protezione avanzata sono valide nei seguenti casi::

- Accesso a SSH in quanto l'utente root è disabilitato.
- utilizzare la sequenza di tasti Ctrl-Alt-Canc per riavviare il server dalla console senza la registrazione disabilitata.
- I reindirizzamenti vengono applicati in tabelle ip per le seguenti porte:
  - Porte TCP 80 e 443 reindirizzate a 5250
  - Porta UDP 514 reindirizzata a 40514
- Il pacchetto GRUB è protetto da password.
- L'installazione aggiunge i seguenti utenti con privilegi minimi:
  - caelmadmin - un account del sistema operativo con diritti di accesso alla console del server CA Enterprise Log Manager
  - caelmservice - account del servizio con cui iGateway e i processi dell'agente vengono eseguiti; non è possibile accedere direttamente con questo account

Reindirizzamento delle porte del firewall per gli eventi syslog

È possibile reindirizzare il traffico delle porte standard su altre porte se si sta utilizzando un firewall tra un agente e il server CA Enterprise Log Manager.

Le migliori prassi di sicurezza dettano i privilegi utente minimi per eseguire i processi delle applicazioni e i daemon. I daemon UNIX e Linux in esecuzione negli account non principali non possono aprire porte inferiori alla 1024. La porta syslog UDP syslog è la 514. Ciò può rappresentare un problema per periferiche come router e switch che non possono utilizzare porte non standard.

Per risolvere questo problema, è possibile configurare il firewall per l'ascolto del traffico in ingresso sulla porta 514 e l'invio al server CA Enterprise Log Manager su una porta diversa. Il reindirizzamento avviene sullo stesso host del listener syslog. Selezionando di utilizzare una porta non standard implica che si dovrà riconfigurare ogni fonte di evento affinché invii i propri eventi a tale porta.

Per reindirizzare il traffico degli eventi attraverso un firewall

1. Effettuare l'accesso come utente principale.
2. Accedere a un prompt dei comandi.
3. Immettere un comando per reindirizzare le porte per il firewall specifico.

   Un esempio delle immissioni da riga di comando per lo strumento di filtraggio del pacchetto netfilter/iptables in esecuzione su un sistema operativo Red Hat Linux assomiglia a quanto segue:

   ```
   chkconfig --level 345

   iptables on iptables -t nat -A PREROUTING -p udp --dport 514 -j REDIRECT --to <nuovaporta>

   service iptables save
   ```

4. Sostituire il valore della variabile *<nuovaporta>* con un numero di porta disponibile superiore a 1024.

   Per altre implementazioni, fare riferimento alle istruzioni per la gestione delle porte fornite dal produttore del firewall.

Installazione del client ODBC

L'installazione di un client ODBC sui sistemi Windows comprende i seguenti passaggi:

1. Verificare di disporre dei permessi necessari e ottenere un codice licenza per il driver del client ODBC (prerequisiti).
2. Installazione del client ODBC
3. Creare un'origine dati tramite l'utilità Windows Data Source (ODBC).
4. Configurare i dettagli di connessione per il client ODBC.
5. Verificare la connessione al database.

Prerequisiti

L'accesso di ODBC all'archivio registro eventi è disponibile solo in CA Enterprise Log Manager r12.1 e versioni successive. Consultare le osservazioni sull'origine dati ODBC per le informazioni necessarie prima di iniziare l'installazione.

Gli utenti di questa funzione devono appartenere a un gruppo di utenti con il privilegio *dataaccess* nel criterio predefinito di accesso ai dati (nel criteri di accesso di CALM). Consultare la *Guida all'amministrazione di CA Enterprise Log Manager r12.1* per ulteriori informazioni sui criteri di accesso.

Per un client ODBC, trovano applicazione i seguenti prerequisiti:

- È necessario disporre dei privilegi di amministratore per installare il client ODBC su un server Windows.
- L'installazione del client ODBC richiede il servizio Installer di Microsoft Windows e visualizza un messaggio se non viene individuato.
- Configurare il servizio server ODBC in CA Enterprise Log Manager, assicurandosi di aver selezionato la casella di controllo Abilita servizio
- Configurare un'origine dati ODBC per i sistemi Windows usando l'utilità Origini dati (ODBC) nel Pannello di controllo.
- È necessario disporre dei diritti per la creazione di file nella directory in cui si desidera installare il client su sistemi UNIX e Linux.

Consultare la matrice di certificazione del supporto di CA Enterprise Log Manager all'indirizzo http://www.ca.com/Support per informazioni sulle piattaforme specifiche supportate per l'uso con la funzione ODBC e JDBC.

Configurazione del servizio server ODBC

Con questa procedura è possibile configurare l'accesso ODBC e JDBC all'archivio registro eventi di CA Enterprise Log Manager .

Per configurare l'accesso ODBC e JDBC

1. Accedere al server CA Enterprise Log Manager come utente amministratore.
2. Accedere alla scheda Amministrazione, quindi fare clic sulla sottoscheda Servizi.

3. Fare clic sul servizio server ODBC per aprire le impostazioni globali o espandere il nodo e selezionare un server CA Enterprise Log Manager specifico.
4. Impostare il valore della porta per il campo Porta servizio, se si decide di utilizzare una porta diversa dal valore predefinito.
5. Specificare se si desidera attivare la connessione SSL per crittografare il trasporto dati tra il client ODBC e il server CA Enterprise Log Manager.

   Nota: le impostazioni della porta del servizio e di abilitazione SSL devono corrispondere sia sul server che sul client ODBC. Il valore predefinito per la porta è 17002 e la crittografia SSL è abilitata. Se queste impostazioni non corrispondono alle impostazioni del client ODBC, i tentativi di connessione non riescono.

Installazione del client ODBC su sistemi Windows

Utilizzare questa procedura per installare il client ODBC su un sistema Windows.

Nota: per installare il client ODBC, è necessario un account amministratore di Windows.

Per installare il client ODBC

1. Individuare la directory del client ODBC nella directory \CA\ELM\ODBC del DVD o dell'immagine di installazione.
2. Fare doppio clic sull'applicazione setup.exe.
3. Rispondere al contratto di licenza e fare clic su Avanti.

   Verrà visualizzata la pagina Scegli percorso di destinazione.
4. Inserire un percorso di destinazione o accettare il percorso predefinito e fare clic su Avanti.

   Verrà visualizzata la finestra di dialogo Seleziona cartella programmi.
5. Selezionare una cartella programmi o accettare la selezione predefinita e fare clic su Avanti.

   Verrà visualizzata la finestra Avvia copia dei file.
6. Fare clic su Avanti per iniziare la copia dei file.

   La finestra di dialogo Stato dell'installazione mostra lo stato di avanzamento dell'installazione. Una volta copiati i file, verrà visualizzato il riquadro InstallShield di completamento della procedura.
7. Fare clic su Fine per completare l'installazione.

Creazione di un'origine dati ODBC su sistemi Windows

Utilizzare questa procedura per creare l'origine dati ODBC necessaria sui sistemi Windows. È possibile creare l'origine dati come DSN utente o DSN di sistema.

Creazione dell'origine dati

1. Accedere al Pannello di controllo di Windows e aprire gli Strumenti di amministrazione.
2. Fare doppio clic sull'utilità Origini dati (ODBC). Verrà visualizzata la finestra di dialogo Amministratore origine dati ODBC:
3. Fare clic su Aggiungi per visualizzare la finestra Crea nuova origine dati.
4. Selezionare la voce Driver ODBC CA Enterprise Log Manager e fare clic su Fine.

   Verrà visualizzatala finestra Impostazione driver ODBC di CA Enterprise Log Manager.
5. Inserire i valori dei campi come descritto nella sezione delle considerazioni sull'origine dati ODBC e fare clic su OK.

Considerazioni sull'origine dati ODBC

Seguono le descrizioni dei campi origine dati di ODBC relativi a CA Enterprise Log Manager:

Nome origine dati

Creare un nome per questa origine dati. Le applicazioni client che intendono utilizzare questi dati usano questo nome per connettersi all'origine dati.

Host di servizio

Specifica il nome del server CA Enterprise Log Manager a cui si connette il client. È possibile utilizzare sia un nome di host che un indirizzo IPv4.

Porta di servizio

Specifica la porta di servizio TCP su cui il server CA Enterprise Log Manager è in ascolto per le connessioni dei client ODBC. Il valore predefinito è 17002. Il valore impostato deve corrispondere all'impostazione del servizio Server ODBC. In caso contrario, si verificherà un errore di connessione.

Origine dati di servizio

Lasciare vuoto questo campo; in caso contrario, si verificherà un errore di connessione.

Crittografia SSL

Indica se utilizzare la crittografia per le comunicazioni fra il client ed il server CA Enterprise Log Manager. Il valore predefinito abilita la crittografia SSL. Il valore impostato deve corrispondere all'impostazione del servizio Server ODBC. In caso contrario, si verificherà un errore di connessione.

Proprietà personalizzate

Specifica le proprietà di connessione da utilizzare con l'archivio registro eventi. Il delimitatore delle proprietà è un punto e virgola senza spazi. I valori predefiniti consigliati sono i seguenti:

querytimeout

Indica il valore di timeout in secondi in assenza di dati restituiti, allo scadere del quale la query verrà chiusa. Segue la sintassi per questa proprietà:

```
querytimeout=300
```

queryfederated

Specifica se eseguire una query federata. Impostando questo valore su false, verrà eseguita una query solo sul server CA Enterprise Log Manager al quale viene eseguita la connessione di database. Segue la sintassi per questa proprietà:

```
queryfederated=true
```

queryfetchrows

Specifica il numero di righe da recuperare in una singola operazione, nel caso in cui la query abbia successo. Il valore minimo è 1 ed il massimo è 5000. Il valore predefinito è 1000. Segue la sintassi per questa proprietà:

```
queryfetchrows=1000
```

offsetmins

Specifica l'offset del fuso orario di questo client ODBC. Un valore pari a 0 utilizza il GMT. È possibile utilizzare questo campo per impostare il proprio offset di fuso orario rispetto al GMT. Segue la sintassi per questa proprietà:

```
offsetmins=0
```

suppressNoncriticalErrors

Indica il comportamento del provider di interfaccia in caso di errori non critici, ad esempio un database o un host che non rispondono.

Segue la sintassi per questa proprietà:

```
suppressNoncriticalErrors=false
```

Verifica della connessione del client ODBC al database

Il client ODBC è installato con uno strumento interattivo SQL Query della riga di comando, ISQL. È possibile utilizzare questo strumento per verificare le impostazioni di configurazione e la connettività tra il client ODBC e il deposito eventi di log di CA Enterprise Log Manager.

Verifica della connessione del client al database

1. Aprire il prompt dei comandi e accedere alla directory dove è installato il client ODBC.
2. Avviare l'utilità ISQL, odbcisql.exe.
3. Inserire il seguente comando per verificare la connessione del client al database:

   ```
   collegare User*Password@DSN_name
   ```

   Usare il nome dell'origine dati creata per questa connessione ODBC al database per il valore DSN_name. Se i parametri della connessione sono corretti, viene restituito un messaggio simile al seguente:

   ```
   SQL: connessione al database in corso: DSN_name
   Tempo trascorso 37 ms.
   ```

Nota: se la password contiene il simbolo @, l'utilità iSQL non verrà eseguita correttamente e leggerà qualsiasi elemento dopo il simbolo "@"come nome DSN. Per evitare questo problema, immettere la password tra virgolette:

```
Connect User*"Password"@DSN_name
```

Verifica del recupero del server dal database

Usare questa query di verifica per stabilire se un'applicazione client ODBC è in grado di recuperare i dati da un archivio di registro eventi di CA Enterprise Log Manager che utilizza la connessione stabilita con il database. Questa procedura sfrutta la stessa utilità ISQL utilizzata per verificare la connessione ODBC.

Nota: non copiare e utilizzare le query SQL fornite nelle query e nei rapporti di CA Enterprise Log Manager per verificare la connessione ODBC. Tali istruzioni SQL devono essere utilizzate solamente dal server CA Enterprise Log Manager con l'archivio di registri eventi. Creare le query SQL ODBC usando le strutture standard secondo lo standard SQL ANSI.

Per verificare il recupero dati del componente server

1. Aprire il prompt dei comandi e accedere alla directory dove è installato il client ODBC.
2. Avviare l'utilità ISQL, odbcisql.exe.
3. Inserire la seguente istruzione SELECT per verificare il recupero dall'archivio registro eventi:

```
select top 5 event_logname, receiver_hostname, SUM(event_count) as Count from
view_event where event_time_gmt < now() and event_time_gmt >
timestampadd(mi,-15,now()) GROUP BY receiver_hostname, event_logname;
```

Installazione del client JDBC

Il client JDBC fornisce l'accesso JDBC attraverso qualsiasi applet, applicazione o server applicazioni Java. Fornisce l'accesso n-tier e point-to-point ad alte prestazioni alle origini dati. Il client è ottimizzato per l'ambiente Java e permette di incorporare la tecnologia Java ed estendere le funzionalità e le prestazioni del sistema esistente.

Il client JDBC viene eseguito su piattaforme a 32 bit e 64 bit. Non è necessario modificare le applicazioni esistenti per consentirne l'esecuzione su piattaforme a 64 bit.

L'installazione del client JDBC comprende i seguenti passaggi:

1. Assicurarsi che sia installato e funzionante un server per applicazioni Web con funzionalità di configurazione del pool di connessione.
2. Ottenere il codice licenza per il driver del client JDBC.
3. Installazione del client JDBC
4. Configurare la connessione al database usando le funzioni di gestione del pool di connessione del server delle applicazioni Web.
5. Verificare la connessione al database.

Prerequisiti del client JDBC

L'accesso di JDBC all'archivio di registro eventi è disponibile solo in CA Enterprise Log Manager r12.1 e versioni successive. È possibile installare il client JDBC su sistemi Windows e UNIX.

Gli utenti di questa funzione devono appartenere a un gruppo di utenti CA Enterprise Log Manager con il privilegio *dataaccess* nel criterio predefinito di accesso ai dati (nel criteri di accesso di CALM). Consultare la *Guida all'amministrazione di CA Enterprise Log Manager r12.1* per ulteriori informazioni sui criteri di accesso.

Per un client JDBC, trovano applicazione i seguenti prerequisiti:

- È necessario disporre dei privilegi di amministratore per installare il client JDBC su un server Windows.
- Verificare che, nella finestra di configurazione del server ODBC, sia selezionata (attivata) la casella di controllo Attiva servizio
- È necessario disporre dei diritti per la creazione di file nella directory in cui si desidera installare il client su sistemi UNIX e Linux.
- Per le applicazioni eseguite in J2SE v 1.4.2.x, impostare le connessioni al database a livello di codice, come definito in una applicazione specifica.
- Per le applicazioni eseguite in J2EE 1.4.2.x e versioni successive, utilizzare un server di applicazioni Web come BEA WebLogic o Red Hat JBoss per configurare la gestione del pool di connessione.

Consultare la matrice di certificazione del supporto di CA Enterprise Log Manager all'indirizzo http://www.ca.com/Support per informazioni sulle piattaforme specifiche supportate per l'uso con la funzione ODBC e JDBC.

Installazione del client JDBC su sistemi Windows

Utilizzare questa procedura per installare il client JDBC su un sistema Windows.

Per installare il driver JDBC

1. Individuare i due file .jar seguenti nel DVD o nell'immagine di installazione dell'applicazione nella directory CA/ELM/JDBC:

   ```
   LMjc.jar
   LMssl14.jar
   ```

2. Copiare i file .jar nella directory desiderata sul server di destinazione e annotare il percorso.

Installazione del client JDBC su sistemi UNIX

Utilizzare questa procedura per installare il client JDBC su un sistema UNIX.

Installazione del client JDBC

1. Individuare i due file .jar seguenti nella directory CA/ELM/JDBC del DVD o dell'immagine di installazione dell'applicazione:

   ```
   LMjc.jar
   LMssl14.jar
   ```

2. Copiare i file .jar nella directory desiderata sul server di destinazione e annotare il percorso.

3. Eseguire il seguente comando (o uno simile) manualmente dalla directory di installazione dopo aver installato il client JDBC per JDBC su UNIX:

   ```
   chmod -R ugo+x file_location
   ```

   Il valore di *file_location* corrisponde alla directory in cui è stato installato il client JDBC. Questo passaggio consente di eseguire gli script di shell forniti con il client installato.

Parametri della connessione JDBC

Varie applicazioni richiedono determinati parametri di connessione per utilizzare il driver del client JDBC. I parametri abituali comprendono quanto segue:

- Stringa di connessione o URL connessione
- Nome di classe

La stringa di connessione JDBC (URL) presenta il seguente formato:

```
jdbc:ca-elm://[CA-ELM_host_name]:[ODBC/JDBCport];ServerDataSource=Default;
```

Il nome della classe del driver JDBC è:

```
com.ca.jdbc.openaccess.OpenAccessDriver
```

Considerazioni sull'URL JDBC

Quando si utilizza il client JDBC per accedere ai dati evento archiviati in CA Enterprise Log Manager, sono necessari sia il classpath che l'URL JDBC. Il Classpath JDBC indica il percorso dei file JAR del driver. L'URL JDBC definisce i parametri utilizzati dalle classi dei file JAR durante il caricamento.

Segue un completo URL JDBC campione:

```
jdbc:ca-
elm://127.0.0.1:17002;encrypted=1;ServerDataSource=Default;CustomProperties=(querytimeout=600;que
ryfederated=true;queryfetchrows=1000;offsetmins=0;suppressNoncriticalErrors=false)
```

Di seguito sono descritti i componenti dell'URL:

jdbc.ca-elm:

Definisce la stringa protocol:subprotocol che indica il driver JDBC fornito con CA Enterprise Log Manager.

//IP Address:Port;

Indica l'indirizzo IP che rappresenta il server CA Enterprise Log Manager contenente i dati ai quali si desidera accedere. Il numero di porta è la porta da utilizzare per le comunicazioni e deve corrispondere all'impostazione configurata nel riquadro Servizio ODBC di CA Enterprise Log Manager. Se le porte non trovano corrispondenza, si verificherà un errore nel tentativo di connessione.

encrypted=0|1;

Stabilisce se si utilizza la crittografia SSL per le comunicazioni tra il client JDBC ed il server CA Enterprise Log Manager. Il valore predefinito è 0, non crittografato, e non è necessario specificarlo nell'URL. L'impostazione encrypted=1 consente di attivare la crittografia. Impostare la connessione sulla crittografia in modo esplicito. Inoltre, tale impostazione deve corrispondere a quanto configurato nella finestra di dialogo del Servizio ODBC CA Enterprise Log Manager; in caso contrario, si verificherà un errore di connessione.

ServerDataSource=Default

Specifica il nome dell'origine dati. Impostare questo valore su *Default* per accedere all'archivio registro eventi di CA Enterprise Log Manager.

CustomProperties=(x;y;z)

Queste proprietà sono identiche alle proprietà di ODBC personalizzate. Se non vengono specificate esplicitamente, verranno applicati i valori predefiniti visualizzati nell'URL di esempio.

Ulteriori informazioni

Considerazioni sull'origine dati ODBC (a pagina 121)

Risoluzione di problemi dell'installazione

È possibile analizzare i seguenti file di log dell'installazione per dare inizio alla risoluzione problemi dell'installazione:

Prodotto	Posizione del file di log
CA Enterprise Log Manager	/tmp/pre-install_ca-elm.log /tmp/install_ca-elm.<*timestamp*>.log /tmp/install_ca-elmagent.<*timestamp*>.log
CA Embedded Entitlements Manager	/opt/CA/SharedComponents/EmbeddedIAM/eiam-install.log
CA Directory	/tmp/etrdir_install.log

L'installazione di CA Enterprise Log Manager copia il contenuto e altri file nel server CA EEM per la gestione. Dalla prospettiva del server CA EEM, i rapporti CA Enterprise Log Manager e altri file vengono *importati*. Se l'installazione non è in grado di connettersi al server CA EEM, l'installazione di CA Enterprise Log Manager continuerà senza l'importazione dei file del contenuto. È possibile importare i file del contenuto manualmente al termine dell'installazione.

Se si riscontrano errori durante l'installazione, è necessario eseguire una o più delle seguenti azioni per completare l'installazione. Ciascuna delle azioni riportate implica l'accesso al server CA Enterprise Log Manager mediante l'account predefinito (caelmadmin), quindi il passaggio degli utenti all'account root.

- Risoluzione di errori di configurazione dell'interfaccia di rete
- Verifica dell'installazione del pacchetto rpm
- Verifica dell'esecuzione del daemon iGateway
- Registrazione dell'applicazione CA Enterprise Log Manager con il server CA EEM
- Acquisizione dei certificati digitali
- Importazione dei rapporti CA Enterprise Log Manager
- Importazione dei file di mapping dei dati
- Importazione dei file di parsing dei messaggi
- Importazione dei file della grammatica evento comune (CEG)
- Importazione dei file di gestione degli agenti comuni

Risoluzione di errori di configurazione dell'interfaccia di rete

Dopo l'installazione, se non è possibile accedere all'interfaccia utente CA Enterprise Log Manager, potrebbe verificarsi un errore di configurazione dell'interfaccia di rete. Esistono due opzioni per risolvere l'errore:

- Rimuovere il cavo di rete fisico e inserirlo in una porta diversa.
- Riconfigurare gli adapter dell'interfaccia di rete logica da una riga di comando.

Per riconfigurare le porte dell'adattatore di rete da una riga di comando

1. Accedere al dispositivo software come utente caelmadmin ed effettuare l'accesso a un prompt dei comandi.
2. Passare all'account dell'utente principale utilizzando il seguente comando:

   ```
   su -
   ```
3. Immettere la password dell'utente principale per confermare l'accesso al sistema.
4. Immettere il seguente comando:

   ```
   system-config-network
   ```

   Interfaccia utente per configurare le visualizzazioni degli adattatori di rete.
5. Impostare le configurazioni delle porte come desiderato e uscire.
6. Riavviare i servizi di rete per applicare le modifiche con il seguente comando:

   ```
   service network restart
   ```

Verifica dell'installazione del pacchetto RPM

È possibile eseguire un controllo rapido dell'installazione verificando che il pacchetto rpm appropriato sia installato.

Per verificare il pacchetto rpm

1. Accedere ad un prompt dei comandi su un server CA Enterprise Log Manager.
2. Accedere con le credenziali dell'account caelmadmin.
3. Passare all'account dell'utente principale con il seguente comando:

   ```
   su - root
   ```

4. Verificare che il pacchetto ca-elm-<versione>.i386.rpm sia installato con il seguente comando:

   ```
   rpm -q ca-elm
   rpm -q ca-elmagent
   ```

   Il sistema operativo restituisce il nome completo del pacchetto se questo è installato.

Registrare il server CA Enterprise Log Manager con il server CA EEM

Sintomo:

Durante l'installazione, l'applicazione CA Enterprise Log Manager non si è registrata correttamente con il server CA EEM. L'applicazione CA Enterprise Log Manager dipende dal server CA EEM per la gestione degli account utente e delle configurazioni dei servizi. Se l'applicazione CA Enterprise Log Manager non è registrata, il software non verrà eseguito correttamente.

Lo script di shell menzionato nella procedura che segue viene copiato automaticamente nella directory indicata durante l'installazione.

Soluzione:

Registrazione manuale dell'applicazione CA Enterprise Log Manager con il server CA EEM.

Per registrare l'applicazione CA Enterprise Log Manager

1. Accedere ad un prompt dei comandi su un server CA Enterprise Log Manager.
2. Accedere con le credenziali dell'account caelmadmin.
3. Passare all'account dell'utente principale con il seguente comando:

   ```
   su -
   ```

4. Navigare fino alla directory /opt/CA/LogManager/EEM.
5. Immettere il comando:

   ```
   ./EEMRegister.sh
   ```

   Lo script di shell registra l'applicazione CA Enterprise Log Manager con il server CA EEM.

Acquisizione di certificati dal server CA EEM

Sintomo:

Durante l'installazione, i certificati digitali non sono stati acquisiti correttamente dal server CA EEM. I certificati digitali sono necessari per avviare ed eseguire l'applicazione CA Enterprise Log Manager.

Lo script di shell menzionato nella procedura che segue viene copiato automaticamente nella directory indicata durante l'installazione.

Soluzione:

Acquisizione manuale dei certificati dal server CA EEM.

Per acquisire i certificati digitali

1. Accedere ad un prompt dei comandi su un server CA Enterprise Log Manager.
2. Accedere con le credenziali dell'account caelmadmin.
3. Passare all'account dell'utente principale con il seguente comando:

   ```
   su -
   ```

4. Navigare fino alla directory /opt/CA/LogManager/EEM.
5. Immettere il comando:

   ```
   ./EEMAcqCert.sh
   ```

   Lo script di shell esegue l'elaborazione necessaria ad acquisire i certificati digitali.

Importazione dei rapporti CA Enterprise Log Manager

Sintomo:

Durante l'installazione, il server CA EEM non ha importato correttamente il contenuto del rapporto dal server CA EEM. È necessario importare il contenuto del rapporto per visualizzare i dati degli eventi dopo che vengono archiviati nell'archivio del registro eventi.

Lo script di shell menzionato nella procedura che segue viene copiato automaticamente nella directory indicata durante l'installazione.

Soluzione:

Importazione manuale del contenuto dei rapporti.

Per importare il contenuto dei rapporti

1. Accedere ad un prompt dei comandi su un server CA Enterprise Log Manager.
2. Accedere con le credenziali dell'account caelmadmin.
3. Passare all'account dell'utente principale con il seguente comando:

   ```
   su -
   ```

4. Navigare fino alla directory /opt/CA/LogManager/EEM/content.
5. Immettere il comando:

   ```
   ./ImportCALMContent.sh
   ```

   Lo script di shell scarica il contenuto dei rapporti dal server CA EEM.

Importazione dei file di mapping dei dati CA Enterprise Log Manager

Sintomo:

Durante l'installazione, il server CA EEM non ha importato correttamente i file del mapping dei dati (DM). È necessario disporre dei file DM per mappare i dati degli eventi in ingresso nell'archivio del registro eventi.

Lo script di shell menzionato nella procedura che segue viene copiato automaticamente nella directory indicata durante l'installazione.

Soluzione:

Importazione manuale dei file DM.

Per importare i file DM

1. Accedere ad un prompt dei comandi su un server CA Enterprise Log Manager.
2. Accedere con le credenziali dell'account caelmadmin.
3. Passare all'account dell'utente principale con il seguente comando:

   ```
   su -
   ```

4. Navigare fino alla directory /opt/CA/LogManager/EEM/content.
5. Immettere il comando:

   ```
   ./ImportCALMDM.sh
   ```

   Lo script di shell importa i file DM dal server CA EEM.

Importazione dei file di analisi dei messaggi CA Enterprise Log Manager

Sintomo:

Durante l'installazione, il server CA EEM non ha importato correttamente i file dell'analisi dei messaggi (.XMP). I file dell'analisi dei messaggi costituiscono un contenuto necessario per la gestione dei registri eventi da varie fonti di eventi attraverso la rete. È necessario disporre dei file di analisi dei messaggi per essere in grado di inserire gli eventi nell'archivio del registro eventi CA Enterprise Log Manager.

Lo script di shell menzionato nella procedura che segue viene copiato automaticamente nella directory indicata durante l'installazione.

Soluzione:

Importazione manuale dei file di analisi dei messaggi.

Importazione dei file di analisi dei messaggi

1. Accedere ad un prompt dei comandi su un server CA Enterprise Log Manager.
2. Accedere con le credenziali dell'account caelmadmin.
3. Passare all'account dell'utente principale con il seguente comando:

   ```
   su -
   ```

4. Navigare fino alla directory /opt/CA/LogManager/EEM/content.
5. Immettere il comando:

   ```
   ./ImportCALMMP.sh
   ```

   Lo script di shell importa il contenuto dei file MP dal server CA EEM.

Importazione dei file della grammatica evento comune (CEG)

Sintomo:

Durante l'installazione, il server CA EEM non ha importato correttamente i file della grammatica evento comune (CEG). La CEG forma lo schema del database alla base dell'archivio del registro eventi. Non sarà possibile archiviare eventi nell'archivio del registro eventi CA Enterprise Log Manager senza i file CEG.

Lo script di shell menzionato nella procedura che segue viene copiato automaticamente nella directory indicata durante l'installazione.

Soluzione:

Importazione manuale dei file CEG.

Per importare i file CEG

1. Accedere ad un prompt dei comandi su un server CA Enterprise Log Manager.
2. Accedere con le credenziali dell'account caelmadmin.
3. Passare all'account dell'utente principale con il seguente comando:

```
su -
```

4. Navigare fino alla directory /opt/CA/LogManager/EEM/content.
5. Immettere il comando:

```
./ImportCALMCEG.sh
```

   Lo script di shell importa i file della grammatica evento comune.

Importazione dei file di gestione degli agenti comuni

Sintomo:

Durante l'installazione, il server CA EEM non ha importato correttamente i file di gestione dell'agente comune. Non è possibile gestire gli agenti nell'interfaccia utente CA Enterprise Log Manager senza questi file.

Lo script di shell menzionato nella procedura che segue viene copiato automaticamente nella directory indicata durante l'installazione.

Soluzione:

Importazione manuale dei file di gestione dell'agente.

Importazione dei file di gestione degli agenti comuni

1. Accedere a un prompt dei comandi sul server CA Enterprise Log Manager.
2. Accedere con le credenziali dell'account caelmadmin.
3. Commutare gli utenti sull'utente di root tramite il seguente comando:

```
su -
```

4. Navigare fino alla directory /opt/CA/LogManager/EEM/content.
5. Immettere il comando:

```
./ImportCALMAgentContent.sh
```

   Lo script di shell importa i file di gestione dell'agente comune.

Importazione dei file di configurazione CA Enterprise Log Manager

Sintomo:

Durante l'installazione, il server CA EEM non ha importato correttamente i file di configurazione. È possibile avviare CA Enterprise Log Manager ma nelle aree di configurazione dei servizi non saranno presenti alcune impostazioni e valori, senza i quali non sarà possibile configurare gli host individuali a livello centralizzato.

Lo script di shell menzionato nella procedura che segue viene copiato automaticamente nella directory indicata durante l'installazione.

Soluzione:

Importazione manuale dei file di configurazione.

Per importare i file di configurazione

1. Accedere a un prompt dei comandi sul server CA Enterprise Log Manager.
2. Accedere con le credenziali dell'account caelmadmin.
3. Commutare gli utenti sull'utente di root tramite il seguente comando:

   ```
   su -
   ```

4. Navigare fino alla directory /opt/CA/LogManager/EEM/content.
5. Immettere il comando:

   ```
   ./ImportCALMConfig.sh
   ```

   Lo script di shell importa i file di configurazione.

Importazione dei file di soppressione e riepilogo

Sintomo:

Durante l'installazione, il server CA EEM non ha importato correttamente i file di soppressione e riepilogo. Senza questi file, non è possibile utilizzare le regole di soppressione e riepilogo in dotazione nell'interfaccia utente di CA Enterprise Log Manager.

Lo script di shell menzionato nella procedura che segue viene copiato automaticamente nella directory indicata durante l'installazione.

Soluzione:

Importare i file di soppressione e riepilogo manualmente.

Per importare i file di soppressione e riepilogo

1. Accedere a un prompt dei comandi sul server CA Enterprise Log Manager.
2. Accedere con le credenziali dell'account caelmadmin.
3. Commutare gli utenti sull'utente di root tramite il seguente comando:

   ```
   su -
   ```

4. Navigare fino alla directory /opt/CA/LogManager/EEM/content.
5. Immettere il comando:

   ```
   ./ImportCALMSAS.sh
   ```

   Lo script di shell importa i file di soppressione e riepilogo.

Importazione dei file del token di analisi

Sintomo:

Durante l'installazione, il server CA EEM non ha importato correttamente i file del token di analisi. Senza questi file non è possibile utilizzare i token di analisi in dotazione nella Procedura guidata di analisi dei messaggi.

Lo script di shell menzionato nella procedura che segue viene copiato automaticamente nella directory indicata durante l'installazione.

Soluzione:

Importazione manuale dei file del token di analisi.

Come importare i file del token di analisi

1. Accedere a un prompt dei comandi sul server CA Enterprise Log Manager.
2. Accedere con le credenziali dell'account caelmadmin.
3. Commutare gli utenti sull'utente di root tramite il seguente comando:

   ```
   su -
   ```

4. Navigare fino alla directory /opt/CA/LogManager/EEM/content.
5. Immettere il comando:

   ```
   ./ImportCALMTOK.sh
   ```

   Lo script di shell importa i file del token di analisi.

Importazione dei file dell'interfaccia utente di CA Enterprise Log Manager

Sintomo:

Durante l'installazione, il server CA EEM non ha importato correttamente i file dell'interfaccia utente. Senza questi file non è possibile visualizzare o utilizzare i valori nei campi del menu a discesa degli intervalli di tempo dinamici.

Lo script di shell menzionato nella procedura che segue viene copiato automaticamente nella directory indicata durante l'installazione.

Soluzione:

Importare i file dell'interfaccia utente manualmente.

Per importare i file dell'interfaccia utente

1. Accedere a un prompt dei comandi sul server CA Enterprise Log Manager.
2. Accedere con le credenziali dell'account caelmadmin.
3. Commutare gli utenti sull'utente di root tramite il seguente comando:

   ```
   su -
   ```

4. Navigare fino alla directory /opt/CA/LogManager/EEM/content.
5. Immettere il comando:

   ```
   ./ImportCALMFlexFiles.sh
   ```

   Lo script di shell importa i file dell'interfaccia utente.

Capitolo 4: Configurazione di utenti e accessi di base

Questa sezione contiene i seguenti argomenti:

Informazioni sugli utenti e gli accessi di base

La configurazione inizia con la configurazione dell'archivio utente, creando uno o più utenti con il ruolo di amministratore predefinito, e i criteri di configurazione della password. Di solito, questa configurazione viene eseguita dal programma di installazione, che può accedere a CA Enterprise Log Manager con le credenziali EiamAdmin. Dopo avere completato questa configurazione, gli utenti definiti come amministratori configurano CA Enterprise Log Manager.

Se la configurazione dell'archivio utente predefinito viene accettata, la configurazione minima che deve essere completata dall'utente EiamAdmin è l'account del primo amministratore. Il primo amministratore può configurare i criteri delle password prima di configurare gli altri componenti di CA Enterprise Log Manager.

Nota: per i dettagli sulla creazione di altri utenti o per la creazione di ruoli personalizzati e criteri di accesso personalizzati, consultare la *Guida all'amministrazione di CA Enterprise Log Manager*.

Configurazione dell'archivio utente

L'archivio utente rappresenta il repository per le informazioni utente globali. È possibile configurare l'archivio utente non appena si installa un server CA Enterprise Log Manager. Solo l'utente EiamAdmin può configurare l'archivio utente; ciò solitamente avviene subito dopo il primo accesso.

Configurare l'archivio utente in uno dei seguenti modi:

- Accettare l'archivio predefinito nel datastore interno

  Nota: l'opzione predefinita potrebbe essere visualizzata come CA Management Database se, durante l'installazione, è stato indicato un CA EEM autonomo.

- Selezionare Riferimento da una directory esterna, che potrebbe essere una directory LDAP come Microsoft Active Directory, Sun One o Novell CA Directory

- Selezione Reference da CA SiteMinder

È possibile configurare l'archivio utente come directory esterna, non è possibile creare nuovi utenti. È possibile aggiungere gruppi di applicazioni, o ruoli, predefiniti e definiti dall'utente, solo alle registrazioni dell'utente globale in sola lettura. È necessario aggiungere nuovi utenti nell'archivio utente esterno e pio aggiungere le autorizzazioni CA Enterprise Log Manager alle registrazioni dell'utente globale.

Accettare l'Archivio utente predefinito

Non è necessario configurare l'archivio utente se si accetta quello predefinito, che è il datastore interno. Questo vale se non è presente un archivio utente esterno a cui fare riferimento.

Per verificare che il repository predefinito sia configurato come archivio utente

1. Accedere a un server CA Enterprise Log Manager come utente con privilegi di amministrazione o con il nome utente EiamAdmin e con la password associata.

2. Fare clic sulla scheda Amministrazione.

   Se si accede come utente EiamAdmin, questa scheda verrà visualizzata automaticamente.

3. Selezionare la sottoscheda Gestione utenti e accessi e fare clic sul pulsante Archivio utente nel riquadro a sinistra.

   Comparirà la Configurazione del server EEM per utenti globali/gruppi globali.

4. Verificare che l'opzione Archivia in un datastore interno sia selezionata.
5. Fare clic su Salva, quindi su Chiudi.

Nota: con l'archivio utente predefinito, è possibile creare nuovi utenti, impostare password temporanee e impostare i criteri delle password.

Ulteriori informazioni:

Pianificazione archivio utente (a pagina 43)

Riferimento a una directory LDAP

Configurare l'archivio utente come riferimento a una directory LDAP quando i dettagli dell'utente globale sono archiviati in Microsoft Active Directory, Sun One, o Novell Directory.

Nota: i dettagli dell'applicazione vengono archiviati nel repository predefinito. Il riferimento a un archivio utente esterno non aggiorna tale archivio utente.

Per fare riferimento a una directory LDAP come archivio utente

1. Accedere a un server CA Enterprise Log Manager come utente con privilegi di amministrazione o come utente EiamAdmin.
2. Fare clic sulla scheda Amministrazione.

   Se si accede come utente EiamAdmin, questa scheda verrà visualizzata automaticamente.

3. Selezionare la sottoscheda Gestione utenti e accessi e fare clic su Archivio utente nel riquadro a sinistra.

   Comparirà la configurazione del server CA EEM per l'Archivio utente.

4. Selezionare Riferimento da una directory esterna.

   Compariranno i campi per la configurazione LDAP.

5. Completare questi campi come pianificato nel foglio di calcolo della directory esterna.

   Considerare il seguente esempio per il binding a oggetti Active Directory, con la seguente stringa di binding:

   Set objUser = Get Object ("LDAP://cn=Bob, cn=Users, ou=Sales, dc=MyDomain, dc=com"), dove cn è il nome comune, ou è l'unità organizzativa e dc è composto da due componenti di dominio che compongono il nome DNS completo. Per il DN utente, inserire:

   ```
   cn=Bob,cn=Users,ou=Sales,dc=MyDomain,dc=com
   ```

6. Fare clic su Salva.

   Salvando questo riferimento le informazioni sull'account utente vengono caricate in CA EEM. Questo rende possibile l'accesso a queste registrazioni utente come utenti globali e l'aggiunta di dettagli a livello di applicazione come il gruppo utente dell'applicazione il nome del ruolo utente.

7. Rivedere lo stato visualizzato per verificare che il bind della directory esterna sia corretto e che i dati vengano caricati.

   Se lo stato visualizza un avviso, fare clic su Aggiorna stato. Se lo stato visualizza un errore, correggere la configurazione, fare clic su Salva e ripetere questo passaggio.

8. Fare clic su Chiudi.

Ulteriori informazioni:

Pianificazione archivio utente (a pagina 43)
Foglio di calcolo directory LDAP esterna (a pagina 45)

Riferimento a CA SiteMinder come archivio utente

Se gli account utente sono già definiti in CA SiteMinder, fare riferimento a questa directory esterna quando si configura l'archivio utente.

Per fare riferimento a CA SiteMinder come archivio utente

1. Accedere a un server CA Enterprise Log Manager come utente con privilegi di amministrazione o come utente EiamAdmin.

2. Fare clic sulla scheda Amministrazione.

   Se si accede come utente EiamAdmin, questa scheda verrà visualizzata automaticamente.

3. Selezionare la sottoscheda Gestione utenti e accessi e fare clic sul pulsante Archivio utente nel riquadro a sinistra.

   Comparirà la configurazione del server CA EEM per l'Archivio utente.

4. Selezionare l'opzione Riferimento da CA SiteMinder.

   Compariranno campi specifici di CA SiteMinder.

   a. Completare questi campi come pianificato nel foglio di calcolo di SiteMinder.

   b. Per visualizzare o modificare le connessioni e le porte utilizzate da CA SiteMinder, fare clic sui puntini di sospensione per visualizzare il riquadro Attributi della connessione.

5. Fare clic su Salva.

   Salvando questo riferimento le informazioni sull'account utente vengono caricate in CA EEM. Questo rende possibile l'accesso a queste registrazioni utente come utenti globali e l'aggiunta di dettagli a livello di applicazione come il gruppo utente dell'applicazione il nome del ruolo utente.

6. Rivedere lo stato visualizzato per verificare che il bind della directory esterna sia corretto e che i dati vengano caricati.

   Se lo stato visualizza un avviso, fare clic su Aggiorna stato. Se lo stato visualizza un errore, correggere la configurazione, fare clic su Salva e ripetere questo passaggio.

7. Fare clic su Chiudi.

Ulteriori informazioni:

Pianificazione archivio utente (a pagina 43)
Foglio di lavoro per CA SiteMinder (a pagina 47)

Configurazione dei criteri delle password

È possibile impostare criteri delle password per garantire che le password che gli utenti creano per sé soddisfino gli standard impostati e che vengano modificate con la frequenza richiesta. Impostare i criteri delle password dopo la configurazione dell'archivio utente interno. Solo l'utente EiamAdmin o un utente a cui è stato assegnato il ruolo di amministratore può impostare o modificare i criteri delle password.

Nota: i criteri delle password CA Enterprise Log Manager non sono validi per gli account utente creati in un archivio utente esterno.

Per configurare criteri delle password

1. Accedere a un server CA Enterprise Log Manager come utente con privilegi di amministrazione o come utente EiamAdmin.
2. Fare clic sulla scheda Amministrazione.

   Se si accede come utente EiamAdmin, questa scheda verrà visualizzata automaticamente.
3. Selezionare la sottoscheda Gestione utenti e accessi e fare clic sul pulsante Criteri password nel riquadro a sinistra.

   Comparirà il riquadro Criteri password.
4. Specificare se permettere che la password corrisponda al nome utente.
5. Specificare se applicare requisiti di lunghezza.
6. Specificare se applicare criteri sui caratteri massimi ripetuti o sul numero minimo o sui caratteri numerici.
7. Specificare i criteri di età e riutilizzo.
8. Verificare le impostazioni, quindi fare clic su Salva.
9. Fare clic su Chiudi.

   I criteri delle password configurati sono validi per tutti gli utenti CA Enterprise Log Manager.

Ulteriori informazioni:

Pianificazione dei criteri delle password (a pagina 48)
Nome utente e una password (a pagina 49)
Età e riutilizzo delle password (a pagina 49)
Lunghezza e formato della password (a pagina 50)

Conservazione di criteri di accesso predefiniti

Se si pianifica di utilizzare i gruppi utente delle applicazioni predefinite, o ruoli, solo con i criteri predefiniti associati, potrebbe presentarsi il rischio che i criteri predefiniti vengano eliminati o risultino danneggiati. Tuttavia, se gli amministratori pianificano la creazione di ruoli definiti dall'utente e di criteri di accesso associati, i criteri predefiniti garantiranno l'accesso, la modifica e saranno vulnerabili a modifiche indesiderate. È una buona prassi conservare un backup dei criteri predefiniti originali che è possibile ripristinare in caso di necessità.

Creare un file di backup contenente ogni tipo di criterio predefinito utilizzando la funzione Esporta. È possibile copiare questi file su un supporto esterno o lasciarli sul disco del server su cui è stata avviata l'esportazione.

Nota: per procedure relative al backup di criteri predefiniti, vedere la *Guida all'amministrazione di CA Enterprise Log Manager*.

Creazione del primo amministratore

Al primo utente creato deve essere assegnato il ruolo di amministratore. Solo gli utenti a cui è assegnato il ruolo di amministratore possono eseguire la configurazione. È possibile assegnare il ruolo di amministratore a un nuovo account utente creato o a un account utente esistente recuperato in CA Enterprise Log Manager.

Utilizzare la seguente procedura:

1. Accedere al server CA Enterprise Log Manager come utente predefinito EiamAdmin.
2. Creare il primo amministratore.

   Il metodo che si utilizza per creare il primo amministratore di CA Enterprise Log Manager dipende dalla configurazione dell'archivio utente.

   - Se si configura CA Enterprise Log Manager per utilizzare l'archivio utente interno, si crea un nuovo account utente con ruolo di amministratore.
   - Se si configura CA Enterprise Log Manager per utilizzare un archivio utente esterno, si deve utilizzare un utente LDAP esistente per il bind della directory. Una volta eseguito il bind a una directory esterna, si recupera dall'archivio utente esterno l'account utente dell'utente a cui assegnare un ruolo CA Enterprise Log Manager. Gli account utente di archivi utente esterni vengono recuperati come utenti globali. Non è possibile modificare le informazioni di un account utente esistente, ma è possibile aggiungere un nuovo gruppo utente o ruolo dell'applicazione CAELM. Per il primo utente, assegnare il ruolo di amministratore.

   Nota: non è possibile creare nuovi utenti da CA Enterprise Log Manager quando si configura un archivio utente esterno.
3. Disconnessione dal server CA Enterprise Log Manager
4. Accedere nuovamente al server CA Enterprise Log Manager con le credenziali del nuovo account utente.

   Quindi sarà possibile eseguire le attività di configurazione.

Creazione di un nuovo account utente

È possibile creare un account utente per ogni persona che utilizzerà CA Enterprise Log Manager. Fornire le credenziali con cui l'utente effettuerà l'accesso per la prima volta e specificare il rispettivo ruolo. I tre ruoli predefiniti includono amministratore, analista e revisore. Quando un nuovo utente a cui è assegnato il ruolo di analista o revisore effettua l'accesso, CA Enterprise Log Manager autentica l'utente con le credenziali salvate e autorizza l'utilizzo di varie funzionalità in base al ruolo assegnato.

Per creare un nuovo utente

1. Accedere al server CA Enterprise Log Manager come utente predefinito EiamAdmin.

   Verrà visualizzata la scheda Amministrazione e la sottoscheda Gestione utenti e accessi.

2. Fare clic su Utenti nel riquadro sinistro.
3. Fare clic su Nuovo utente a sinistra della cartella Utenti.

   Sul lato destro della finestra viene visualizzata la schermata contenente i dettagli del nuovo utente.

4. Digitare un nome utente nel campo Nome utente. I nomi utente non effettuano la distinzione tra maiuscole e minuscole.
5. Fare clic su Aggiungi informazioni su utente applicazione.
6. Selezionare il ruolo associato alle attività che verranno eseguite da questo utente. Utilizzare il controllo pilota per spostarlo nell'elenco Gruppi utente selezionati.
7. Fornire i valori dei campi rimanenti nella schermata come necessario. È necessario fornire una password che distingua maiuscole e minuscole con conferma nella casella del gruppo di autenticazione.
8. Fare clic prima su Salva, quindi su Chiudi.

Ulteriori informazioni:

Assegnazione di un ruolo a un utente globale (a pagina 148)

Assegnazione di un ruolo a un utente globale

È possibile cercare un account utente esistente e assegnare il gruppo utente dell'applicazione per il ruolo che si desidera assegnare a quella persona. Se si fa riferimento a un archivio utente esterno, la ricerca restituisce record globali caricati da quell'archivio utente. Se l'archivio utente configurato è quello di CA Enterprise Log Manager, la ricerca restituisce i record creati per gli utenti in CA Enterprise Log Manager.

Soltanto gli amministratori sono autorizzati a modificare gli account utente.

Per assegnare un ruolo (o gruppo utente dell'applicazione) a un utente esistente

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Utenti nel riquadro sinistro.

   Vengono visualizzati i riquadri Ricerca utenti e Utenti.
3. Selezionare Utenti globali, inserire un criterio di ricerca e fare clic su Vai a.

   Se si stanno cercando account utente caricati, il riquadro Utenti mostra il percorso e le etichette percorso rispecchiano la directory esterna di riferimento.

   Importante: specificare sempre i criteri quando si esegue una ricerca, per evitare di visualizzare tutte le voci dell'archivio utente esterno.
4. Selezionare un utente globale senza appartenenza ad alcun gruppo applicazione CA Enterprise Log Manager.

   Viene visualizzata la pagina utente con il nome della cartella, i dettagli sull'utente globale e, laddove applicabile, l'appartenenza al gruppo globale.
5. Fare clic su Aggiungi dettagli utente applicazione.

   Il riquadro dettagli utente "CAELM" si espande.
6. Selezionare il gruppo desiderato da Gruppi utente disponibili e fare clic sulla freccia a destra.

   Il gruppo selezionato viene visualizzato nella casella Gruppi utente selezionati.
7. Fare clic su Salva.

8. Verificare che il gruppo sia stato aggiunto.
    a. Nel riquadro Ricerca utenti, fare clic su Dettagli utente applicazione, quindi su Vai a.
    b. Verificare che il nome del nuovo utente dell'applicazione venga visualizzato tra i risultati.
9. Fare clic su Chiudi.

Capitolo 5: Configurazione dei servizi

Questa sezione contiene i seguenti argomenti:

Fonti e configurazioni degli eventi

La maggior parte delle reti dispone di periferiche basate su Windows e su syslog i cui registri eventi devono essere raccolti, archiviati, monitorati e controllati. La rete può disporre anche di altri tipi di periferiche, incluse applicazioni, database, lettori di badge, periferiche biometriche o registratori CA Audit e iRecorder esistenti. I servizi, gli adapter, gli agenti e i connettori CA Enterprise Log Manager rappresentano le configurazioni necessarie per connettersi a queste origini eventi e ricevere dati di evento.

I servizi CA Enterprise Log Manager includono le seguenti aree per le configurazioni e le impostazioni:

- Configurazioni globali
- Filtri e impostazioni globali
- Impostazioni archivio registro eventi
- Impostazioni server ODBC
- Impostazioni server rapporti
- Configurazione Modulo di sottoscrizione
- Pannello di accesso allo stato del sistema

Le configurazioni dei servizi possono essere globali, ovvero possono riguardare tutti i server CA Enterprise Log Manager installati con un unico nome di istanza dell'applicazione nel server di gestione. Le configurazioni possono essere anche locali, riguardando solo un server selezionato. Le configurazioni vengono archiviate nel server di gestione con una copia locale sul server di raccolta CA Enterprise Log Manager. In questo modo, se la connettività di rete viene perduta o il server di gestione è inattivo per qualsiasi motivo, la registrazione degli eventi continua senza interruzione sui server di raccolta.

Il pannello di accesso allo stato del sistema fornisce gli strumenti che hanno effetto su un server CA Enterprise Log Manager e i relativi servizi e per la raccolta di informazioni per l'assistenza. La Guida all'amministrazione e la guida in linea contengono ulteriori informazioni su questa area.

Modificare le configurazioni globali

È possibile impostare le configurazioni globali per tutti i servizi. Se si tenta di salvare valori non inclusi nell'intervallo consentito, per impostazione predefinita verrà utilizzato il valore massimo o minimo, a seconda dei casi. Molte delle impostazioni sono interdipendenti.

Per modificare le impostazioni globali

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.

   Viene visualizzato l'Elenco servizi.

2. Fare clic su Configurazione globale nell'Elenco servizi.

   Verrà visualizzato il riquadro dei dettagli Configurazione di servizio globale.

3. Modificare una delle seguenti impostazioni di configurazione:

   Intervallo di aggiornamento

   Indica la frequenza, in secondi, con cui i componenti del server applicheranno gli aggiornamenti di configurazione.

   Minimo: 30

   Massimo: 86400

Timeout di sessione

Specifica la lunghezza massima di una sessione inattiva. Se viene abilitata la funzione di aggiornamento automatico, la sessione non scade mai.

Minimo: 10

Massimo: 60

Consenti aggiornamento automatico

Consente agli utenti di aggiornare automaticamente i report o le query. Questa impostazione consente agli amministratori di disabilitare globalmente l'aggiornamento automatico.

Frequenza di aggiornamento automatico

Specifica, in minuti, l'intervallo di tempo tra gli aggiornamenti della visualizzazione del rapporto. Questa impostazione dipende dalla selezione di Consenti aggiornamento automatico.

Minimo: 1

Massimo: 600

Abilita aggiornamento automatico

Imposta l'aggiornamento automatico in tutte le sessioni. Per impostazione predefinita, l'aggiornamento automatico non è abilitato.

Per visualizzare gli avvisi è necessario effettuare l'autenticazione

Impedisce ai revisori o ai prodotti di terze parti di visualizzare i feed RSS di avviso. Questa funzione è attivata per impostazione predefinita.

Rapporto predefinito

Consente di specificare il rapporto predefinito.

Abilita avvio del rapporto predefinito

Visualizza il rapporto predefinito facendo clic sulla scheda Rapporti. Questa funzione è attivata per impostazione predefinita.

4. Modificare una delle seguenti impostazioni relative a rapporti e tag delle query:

Nascondi tag di rapporto

Impedisce la visualizzazione dei tag specificati negli elenchi di tag. Nascondendo i tag di rapporto, sarà più semplice visualizzare i rapporti disponibili.

Nascondi tag delle query

Consente di nascondere i tag selezionati. I tag nascosti non verranno visualizzati nell'elenco principale delle query o nell'elenco delle query di pianificazione degli avvisi. Nascondendo i tag di query, sarà possibile personalizzare la visualizzazione delle query disponibili.

5. Modificare una delle seguenti impostazioni di profilo:

   Attivazione profilo predefinito

   Consente di impostare il profilo predefinito.

   Profilo predefinito

   Indica il profilo predefinito.

   Nascondi profili

   Consente di nascondere i profili selezionati. I profili nascosti non verranno visualizzati quando si aggiorna l'interfaccia o quando scade l'intervallo di aggiornamento. Nascondendo i profili, sarà possibile personalizzare la visualizzazione dei profili disponibili.

   Nota: fare clic su Reimposta per ripristinare i valori dell'ultimo salvataggio. Sarà possibile ripristinare una o più modifiche, finché non le si salva. Una volta salvate le modifiche, sarà necessario reimpostarle singolarmente.

6. Fare clic su Salva.

Utilizzo di impostazioni e filtri globali

È possibile definire filtri e impostazioni globali come parte della configurazione del proprio server CA Enterprise Log Manager. Le impostazioni globali vengono salvate solo per la sessione corrente e non persistono dopo la disconnessione dal server, a meno che venga selezionata l'opzione Utilizza come predefinite.

Un *filtro rapido* globale controlla l'intervallo iniziale in cui eseguire il rapporto, offre filtraggio del testo con corrispondenza semplice e permette di utilizzare campi specifici e i relativi valori per modificare i dati visualizzati in un rapporto.

Un *filtro avanzato* globale permette di utilizzare la sintassi e gli operatori SQL per esaminare ulteriormente i dati del rapporto. Le impostazioni globali permettono di impostare un fuso orario e di utilizzare query speciali che recuperano i dati da altri server CA Enterprise Log Manager in una federazione, oltre ad abilitare l'aggiornamento automatico dei rapporti durante la visualizzazione.

Impostare filtri globali adatti all'utilizzo in aree di rapporto multiple. Impostando opzioni che limitano i filtri globali, è possibile controllare la quantità di dati mostrata in un rapporto. Le attività iniziali riguardanti filtri e impostazioni globali includono le seguenti:

- Configurare i filtri rapidi globali per fornire un periodo iniziale che interessi i rapporti visualizzati da questo server CA Enterprise Log Manager;
- Selezionare query federate nella scheda Impostazioni per visualizzare i dati dai server CA Enterprise Log Manager federati con questo server;
- Decidere se aggiornare automaticamente i rapporti;
- Impostare l'intervallo con cui aggiornare i dati nel rapporto.

Nota: impostando il filtro globale in modo troppo limitato o specifico, si potrebbe impedire la visualizzazione dei dati in alcuni rapporti.

Ulteriori informazioni sui filtri globali e sul loro utilizzo sono disponibili nella Guida in linea.

Ulteriori informazioni:

Modificare le configurazioni globali (a pagina 152)

Selezione dell'utilizzo di query federate

È possibile specificare se si desidera eseguire query su dati federati. Se si ha intenzione di utilizzare più di un server CA Enterprise Log Manager in una rete federata, è possibile selezionare la casella di controllo Usa query federate. Questa opzione permette di raccogliere dati degli eventi al fine della creazione di rapporti da tutti i server CA Enterprise Log Manager federati in (che agiscono come figli di) questo server CA Enterprise Log Manager.

È inoltre possibile scegliere di disattivare le query federate per una query specifica, se si desidera osservare i dati solo dal server CA Enterprise Log Manager corrente.

Per impostare l'utilizzo delle query federate

1. Accedere al server CA Enterprise Log Manager.
2. Fare clic sul pulsante Mostra/Modifica filtri globali.

   Il pulsante si trova alla destra del nome del server CA Enterprise Log Manager corrente e appena sopra alle schede principali.
3. Fare clic sulla scheda Impostazioni.

4. Specificare se utilizzare le query federate.

   Se si disattivano le opzioni delle query federate selezionate, i rapporti visualizzati *non* conterranno dati degli eventi dai server configurati come figli di questo server.

Ulteriori informazioni:

Configurazione di una federazione CA Enterprise Log Manager (a pagina 225)
Configurazione di un server CA Enterprise Log Manager come server figlio (a pagina 226)

Configurazione dell'intervallo di aggiornamento globale

È possibile definire l'intervallo con cui i servizi CA Enterprise Log Manager controllano se la configurazione ha subito modifiche. Il valore predefinito, dopo l'installazione, è di cinque minuti e viene espresso in secondi. L'impostazione di questo valore a intervalli molto lunghi può provocare il ritardo nell'applicazione delle modifiche alla configurazione.

Per configurare l'intervallo di aggiornamento

1. Accedere al server CA Enterprise Log Manager e fare clic sulla scheda Amministrazione.
2. Fare clic sulla scheda Servizi e selezionare il nodo del servizio Configurazione globale.
3. Immettere un nuovo valore per l'intervallo di aggiornamento.

   Il valore predefinito e consigliato è 300 secondi.

Informazioni sui filtri locali

I filtri locali operano su un rapporto live durante la sua visualizzazione e ignorano temporaneamente le impostazioni globali. È possibile utilizzare i filtri locali per trattare i dati in un rapporto, per aiutare a risolvere problemi di sicurezza e a trovare un rapporto specifico in un elenco di rapporti generati. Le attività di configurazione locale includono quanto segue:

- Impostazione di un nuovo filtro per un rapporto live durante la sua visualizzazione
- Impostazione di un filtro in un elenco di rapporti generati per visualizzare un set secondario dell'elenco per nome e tipo di rapporto

La guida in linea dispone di maggiori informazioni sull'impostazione di filtri locali durante la visualizzazione di un rapporto o di un elenco di rapporti.

Configurazione dell'archivio registro eventi

L'archivio registro eventi è il database proprietario di base che contiene i registri eventi raccolti. Le opzioni di configurazione impostate per il servizio archivio registro eventi possono essere globali o locali e riguardano la memorizzazione e l'archiviazione degli eventi da parte del server CA Enterprise Log Manager. La procedura di configurazione dell'archivio registro eventi include quanto segue:

- Comprendere il servizio archivio registro eventi
- Comprendere la gestione dei file di archivio da parte dell'archivio registro eventi
- Configurazione dei valori globali e locali dell'archivio registro eventi

  Questa fase comprende l' impostazione della dimensione del database, i valori di base per la memorizzazione del file archivio, le regole di riepilogo, le regole di soppressione, le relazioni di federazione, le impostazioni della correlazione, i controlli di integrità dei dati e le opzioni di archiviazione automatica.

CA Enterprise Log Manager chiude automaticamente i file del database attivo e crea file di archivio quando i database attivi raggiungono la capacità definita per questo servizio. Quindi CA Enterprise Log Manager apre nuovi file attivi per continuare le operazioni di registrazione di eventi. È possibile configurar opzioni di auto-archiviazione per gestire questi file, ma solo come configurazione locale per ogni server CA Enterprise Log Manager.

Informazioni sul servizio archivio registro eventi

Il servizio archivio registro eventi gestisce le interazioni dei database come il seguente:

- Inserimento di nuovi eventi nel database (hot) corrente
- Recupero di eventi da database federati locali e remoti per query e rapporti
- Creazione di nuovi database quando il database corrente è completo
- Creazione di nuovi file di archivio ed eliminazione dei vecchi file di archivio
- Gestione della cache delle query dell'archivio
- Applicazione delle regole di riepilogo e di soppressione selezionate
- Applicazione delle regole di inoltro eventi selezionate
- Definizione dei server CA Enterprise Log Manager che agiscono come figli federati di questo server CA Enterprise Log Manager

Informazioni sui file di archivio

Il server CA Enterprise Log Manager crea automaticamente file di database, chiamati file di *archivio*, quando un database hot raggiunge le impostazioni del Numero massimo di righe specificate all'interno del servizio archivio registro eventi. I file di database hot non sono compressi.

Quando si configura l'auto-archiviazione da un server di raccolta in un server di rapporto, i database warm sul server di raccolta vengono eliminati dopo che i database vengono copiati sul server di rapporto. L'opzione Numero massimo di giorni di archiviazione non è valida in questo caso.

Quando si configura l'auto-archiviazione da un server di rapporto a un server di archiviazione remoto, i database warm sul server di rapporto non vengono eliminati dopo essere stati copiati sul server di archiviazione remoto. Al contrario, questi database warm vengono conservati sul server di rapporto fino a quando viene raggiunto il valore specificato in Numero massimo di giorni di archiviazione. A questo punto vengono *eliminati*. Tuttavia, una registrazione di questi database cold eliminati viene conservata in modo che si possa interrogare il database degli archivi per i dettagli, nel caso tali informazioni fossero necessarie per eseguire un ripristino.

Quando si stabilisce come impostare il Numero massimo di giorni di archiviazione, tenere in considerazione la quantità di spazio su disco disponibile sul server di rapporto. La configurazione dello Spazio di archiviazione su disco imposta la soglia. Se lo spazio su disco disponibile scende al di sotto della percentuale impostata, i dati del registro eventi vengono eliminati per creare più spazio anche quando il Numero massimo di giorni di archiviazione non è trascorso.

Quando non si configura l'auto-archiviazione da un server di rapporto a un server di archiviazione remoto, è necessario eseguire manualmente il backup dei database warm e spostare manualmente la copia in una posizione di archiviazione remota con una frequenza superiore a quella del Numero massimo di giorni di archiviazione configurato. In caso contrario, si rischia di perdere i dati. Si consiglia di eseguire quotidianamente il backup dei file di archivio per evitare una potenziale perdita dei dati e per mantenere una quantità adeguata di spazio su disco. Il servizio archivio registro eventi gestisce la sua cache interna per le query sui database archiviati per migliorare le prestazioni quando vengono eseguite query ripetute o molto ampie.

Ulteriori informazioni sul funzionamento dei file archivio è disponibile nella *Guida all'amministrazione CA Enterprise Log Manager*.

Ulteriori informazioni:

Esempio: archiviazione automatica fra tre server (a pagina 173)

Informazioni sull'archiviazione automatica

La gestione dei registri eventi archiviati richiede una gestione accurata dei backup e dei file ripristinati. La configurazione del servizio di archiviazione dei registri eventi fornisce una posizione centralizzata per configurare e ottimizzare le dimensioni e la conservazione dei database interni e per impostare opzioni di archiviazione automatica. CA Enterprise Log Manager fornisce i seguenti script per aiutare nelle seguenti attività:

- backup-ca-elm.sh
- restore-ca-elm.sh
- monitor-backup-ca-elm.sh

Nota: l'utilizzo di questi script da per scontato che sia stato stabilita l'autenticazione non interattiva tra i due server utilizzando chiavi RSA.

Gli script di *backup* e *ripristino* utilizzano l'utilità LMArchive per facilitare la copia di database warm in o da host remoti. Gli script aggiornano automaticamente i file di catalogo appropriati al termine dell'attività. È possibile eseguire la copia in server remoti o in altri server CA Enterprise Log Manager. Se l'host remoto in cui si inviano i file è un server CA Enterprise Log Manager, gli script aggiornano automaticamente i file del catalogo anche nel server di ricezione. Gli script eliminano anche i file di archivio dalla macchina locale per evitare la duplicazione nei rapporti federati. Ciò garantisce che i dati siano disponibili per le query e i rapporti. L'archiviazione all'esterno del sistema viene chiamata archivio cold. È possibile ripristinati i file spostati all'archivio cold per query e rapporti.

Lo script di *monitoraggio* esegue automaticamente lo script di backup utilizzando le impostazioni specificate nella porzione dell'archiviazione automatica della configurazione del servizio dell'archivio registro eventi.

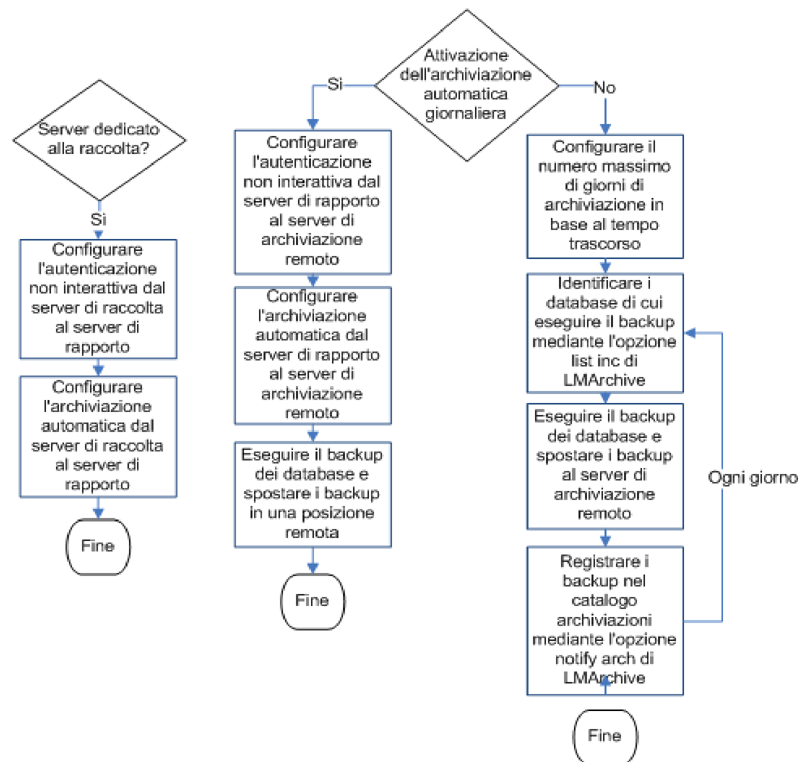
Ulteriori informazioni:

Esempio: archiviazione automatica fra tre server (a pagina 173)

Spostamento del database e diagramma di flusso delle strategie di backup

È possibile eseguire contemporaneamente la raccolta di eventi e la creazione di rapporti su ogni server CA Enterprise Log Manager oppure è possibile dedicare server diversi alla raccolta e ai rapporti. Se dei server sono stati dedicati alla raccolta, ogni ora è richiesto uno spostamento automatico dal server di raccolta al server di rapporto; in caso contrario, non è applicabile. Se non si dispone di ruoli server dedicati, interpretare i riferimenti del diagramma di flusso "da server di rapporto a archiviazione remota" come "da CA Enterprise Log Manager non dedicato a archiviazione remota."

Una strategia di backup implica la presenza di due copie di ogni database, in cui uno viene considerato il backup. È possibile raggiungere questo obiettivo con o senza l'archiviazione automatica in un server di archiviazione remoto. La strategia di backup archiviazione automatica viene riflessa nei database originali sul server di archiviazione remoto e i backup in una posizione esterna. La strategia di backup senza archiviazione automatica viene riflessa nei database originali sul server CA Enterprise Log Manager e i backup in un server di archiviazione remoto. Qualora sia possibile archiviare il database sul server CA Enterprise Log Manager in cui sono stati inizialmente archiviati dipende dallo spazio disponibile per l'archiviazione a lungo termine e dai criteri di archiviazione. Se questi criteri vengono soddisfatti, la decisione viene lasciata alle preferenze personali.



Configurazione dell'autenticazione non interattiva per archiviazione automatica

È possibile configurare l'archiviazione automatica tra server con ruoli diversi. Ad esempio:

- Da uno o più server di raccolta a un singolo server di rapporto.
- Da uno o più server di rapporto a un singolo server di archiviazione remota.

Prima di configurare l'archiviazione automatica da un server a un altro, configurare l'autenticazione *ssh* non interattiva dal server di origine al server di destinazione. *Non interattiva* significa che un server può trasferire file su di un altro senza richiedere alcuna password.

- Se si dispone di soli tre server, un server di raccolta, un server di rapporto e un server di archiviazione remoto, è necessario configurare l'autenticazione non interattiva due volte:
  - Dal server di raccolta al server di rapporto
  - Dal server di rapporto al server di archiviazione remota.
- Se si dispone di sei server con quattro server di raccolta, un server di rapporto e un server di archiviazione remoto, è necessario configurare l'autenticazione non interattiva cinque volte:
  - Dal server di raccolta 1 al server di rapporto.
  - Dal server di raccolta 2 al server di rapporto.
  - Dal server di raccolta 3 al server di rapporto.
  - Dal server di raccolta 4 al server di rapporto.
  - Dal server di rapporto al server di archiviazione remota.

La configurazione dell'autenticazione ssh non interattiva tra due server utilizza le coppie di chiavi RSA, una chiave privata e una chiave pubblica. Copiare prima la chiave pubblica generata nel server di destinazione come authorized_keys. Quando vengono configurate più istanze di autenticazione non interattiva per lo stesso server di rapporto di destinazione, copiare le chiavi pubbliche aggiuntive per i nomi file univoci per evitare di sovrascrivere il file originale authorized_keys. Questi nomi file vengono concatenati a authorized_keys. Ad esempio, se viene aggiunto authorized_keys_ELM-C2 e authorized_keys_ELM-C3 al file authorized_keys da ELM-C1.

Esempio: Configurazione dell'autenticazione non interattiva per hub e spoke

L'esistenza di autenticazione non interattiva tra due server è un prerequisito per l'archiviazione automatica dal sistema di origine al server di destinazione. Uno scenario comune per la configurazione dell'autenticazione non interattiva è uno scenario in cui più server di origine dedicati alla raccolta dispongono di un server di destinazione comune dedicato alla rapporto/gestione. Questo esempio presuppone una federazione CA Enterprise Log Manager di medie dimensioni con un server di rapporto/gestione (hub), quattro server di raccolta (spoke) e un server di archiviazione remoto. I nomi per i server in ciascun ruolo server sono i seguenti:

- Server di rapporto/gestione CA Enterprise Log Manager: ELM-RPT
- Server di raccolta CA Enterprise Log Manager: ELM-C1, ELM-C2, ELM-C3, ELM-C4
- Server di archiviazione remoto:RSS.

Le procedure per l'abilitazione dell'autenticazione non interattiva per la federazione CA Enterprise Log Manager sono le seguenti:

1. Dal primo server di raccolta, generare una coppia di chiavi RSA come caelmservice e copiare la chiave pubblica come authorized_keys nella directory /tmp sul server di rapporto di destinazione.
2. Da ciascun eventuale server di raccolta aggiuntivo, generare una coppia di chiavi RSA e copiare la chiave pubblica come authorized_keys_n, dove n identifica in modo univoco l'origine.
3. Dalla directory /tmp, il server di rapporto concate il contenuto dei file della chiave pubblica per authorized_keys originale. Creare una directory .ssh e modificare la proprietà della directory a caelmservice, spostare authorized_keys alla directory .ssh e impostare la proprietà del file della chiave e delle autorizzazioni necessarie.
4. Verificare che l'autenticazione non interattiva esista tra i server di raccolta e il server di rapporto.
5. Dal server di archiviazione remoto, creare una struttura di directory per la directory .ssh, dove l'impostazione predefinita è /opt/CA/LogManager. Creare una directory .ssh sul sistema di destinazione e modificare la proprietà a caelmservice.
6. Dal server di rapporto, generare una coppia di chiavi RSA come caelmservice e copiare la chiave pubblica come authorized_keys nella directory /tmp sul server di archiviazione remoto di destinazione.

7. Dal server di archiviazione remoto, spostare authorized_keys dalla directory /tmp alla directory .ssh e impostare la proprietà del file della chiave a caelmservice con le autorizzazioni necessarie.
8. Verificare che l'autenticazione non interattiva esista tra il server di rapporto e il server di archiviazione remoto.

Configurazione delle chiavi per la prima coppia raccolta/rapporto

la configurazione dell'autenticazione non interattiva per un'architettura hub e spoke inizia con la generazione di una coppia di chiavi RSA pubbliche/private su un server di raccolta e con la copia della chiave pubblica per il server di rapporto. Copiare il file della chiave pubblica con nome *.authorized_keys.* Supponiamo che questa chiave sia la prima chiave pubblica copiata per il server di rapporto specificato.

Per generare una coppia di chiavi nel primo server di raccolta e copiare la chiave pubblica in un server di rapporto

1. Accedere a ELM-C1attraverso ssh come utente caelmadmin.
2. Commutare gli utenti su root.

   ```
   su –
   ```

3. Commutare gli utenti sull'account caelmservice.

   ```
   su – caelmservice
   ```

4. Generare la coppia di chiavi RSA utilizzando il seguente comando:

   ```
   ssh-keygen –t rsa
   ```

5. Premere Invio per accettare il valore predefinito per ognuno dei seguenti prompt:
   - Specificare il file in cui salvare la chiave (/opt/CA/LogManager/.ssh/id_rsa):
   - Immettere la passphrase oppure lasciare il campo vuoto:
   - Immettere nuovamente la stessa passphrase:
6. Passare alla directory /opt/CA/LogManager.
7. Modificare i permessi della directory .ssh con il seguente comando:

   ```
   chmod 755 .ssh
   ```

8. Accedere a .ssh, in cui è salvata la chiave id_rsa.pub.

   ```
   cd .ssh
   ```

9. Copiare il file id_rsa.pub in ELM-RPT, il server di destinazione CA Enterprise Log Manager, utilizzando il seguente comando:

   ```
   scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys
   ```

   Verrà creato il file authorized_keys sul server di rapporto con il contenuto della chiave pubblica.

Configurazione delle chiavi per una coppia aggiuntiva raccolta/rapporto

Il secondo passaggio della configurazione dell'autenticazione non interattiva per un'architettura hub e spoke consiste nella generazione di una coppia di chiavi RSA su ciascuno dei server di raccolta e nella copia di tale coppia nella directory /tmp del server di rapporto comune come authorized_keys_n, dove n fa riferimento in modo univoco al server di raccolta di origine.

Per generare una coppia di chiavi RSA in server di raccolta aggiuntivi e copiare la chiave pubblica in un server di rapporto comune:

1. Accedere al secondo server di raccolta ELM-C2 mediante ssh come caelmadmin.
2. Commutare gli utenti su root.
3. Far passare gli utenti all'account caelmservice.

   ```
   su – caelmservice
   ```

4. Generare la coppia di chiavi RSA utilizzando il seguente comando:

   ```
   ssh-keygen –t rsa
   ```

5. Premere Invio per accettare il valore predefinito per ognuno dei seguenti prompt:
   - Specificare il file in cui salvare la chiave (/opt/CA/LogManager/.ssh/id_rsa):
   - Immettere la passphrase oppure lasciare il campo vuoto:
   - Immettere nuovamente la stessa passphrase:
6. Modificare la directory in: /opt/CA/LogManager.
7. Modificare i permessi della directory .ssh con il seguente comando:

   ```
   chmod 755 .ssh
   ```

8. Accedere a .ssh, in cui è salvata la chiave id_rsa.pub.

9. Copiare il file id_rsa.pub nel server di destinazione CA Enterprise Log Manager ELM-RPT utilizzando il seguente comando:

   ```
   scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C2
   ```

   Verrà creato il file authorized_keys_ELM-C2 sul server di rapporto con il contenuto della chiave pubblica.

10. Digitare yes seguito dalla password caelmadmin di ELM-RPT
11. Digitare exit.
12. Ripetere i passaggi 1-11 di questa procedura sul server di raccolta ELM-C3. Per il passaggio 9, specificare le seguenti informazioni:

    ```
    scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C3
    ```

13. Ripetere i passaggi 1-11 di questa procedura sul server di raccolta ELM-C4. Per il passaggio 9, specificare le seguenti informazioni:

    ```
    scp id_rsa.pub caelmadmin@ELM-RPT:/tmp/authorized_keys_ELM-C4
    ```

Creazione di un file della chiave pubblica sul server di rapporto e impostazione della proprietà del file

In questo scenario sono state generate coppie di chiavi in ogni server di raccolta e è stata copiata una parte della chiave pubblica parte nel server di rapporto come i seguenti file:

- authorized_keys
- authorized_keys_ELM-C2
- authorized_keys_ELM-C3
- authorized_keys_ELM-C4

Il passaggio 3 consiste nella concatenazione dei file, nello spostamento del file della chiave pubblica RSA nella directory corretta e l'impostazione della proprietà del file e della directory a caelmservice.

Per creare un file della chiave pubblica nella directory corretta sul server di rapporto e impostare la proprietà del file

1. Accedere al server di rapporto CA Enterprise Log Manager mediante ssh come utente caelmadmin.
2. Commutare gli utenti su root.

3. Spostarsi alla cartella CA Enterprise Log Manager:

```
cd /opt/CA/LogManager
```

4. Creare la cartella .ssh.

```
mkdir .ssh
```

5. Assegnare la proprietà della nuova cartella all'utente e al gruppo caelmservice:

```
chown caelmservice:caelmservice .ssh
```

6. Passare alla directory /tmp
7. Aggiungere il contenuto delle chiavi pubbliche dai server di raccolta ELM-C2, ELM-C3 e ELM-C4 per il file authorized_keys che contiene la chiave pubblica da ELM-C1.

```
cat authorized_keys_ELM-C2 >> chiavi autorizzate
cat authorized_keys_ELM-C3 >> chiavi autorizzate
cat authorized_keys_ELM-C4 >> chiavi autorizzate
```

8. Modificare la directory in: opt/CA/LogManager/.ssh
9. Copiare il file authorized_keys dalla cartella /tmp alla cartella attuale .ssh:

```
cp /tmp/authorized_keys .
```

10. Modificare la proprietà del file authorized_keys per l'account caelmservice:

```
chown caelmservice:caelmservice authorized_keys
```

11. Modificare le autorizzazioni sul file:

```
chmod 755 authorized_keys
```

    755 stabilisce l'accesso in lettura ed esecuzione per tutti gli utenti e l'accesso in lettura, scrittura ed esecuzione per il proprietario del file

Questa fase definisce il completamento della configurazione di autenticazione senza l'uso della password tra i server di raccolta e il server di rapporto.

Convalida dell'autenticazione non interattiva tra i server di raccolta e i server di rapporto

È possibile convalidare la configurazione dell'autenticazione non interattiva tra i server di origine e di destinazione di entrambe le fasi dell'archiviazione automatica.

Per convalidare la configurazione tra i server di raccolta e dei rapporti

1. Accedere al server di raccolta ELM-C1attraverso ssh come caelmadmin.
2. Commutare gli utenti su root.
3. Commutare gli utenti sull'account caelmservice.

   ```
   su – caelmservice
   ```

4. Inserire il comando riportato di seguito:

   ```
   ssh caelmservice@ELM-RPT
   ```

   L'accesso a ELM-RPT senza l'immissione di una passphrase confermerà l'autenticazione non interattiva tra ELM-C1 e ELM-RPT.

5. Accedere a ELM-C2 e ripetere.
6. Accedere a ELM-C3 e ripetere.
7. Accedere a ELM-C4 e ripetere.

Creazione di una struttura di directory con proprietà sul server di archiviazione remoto

Questa procedura presuppone che il server di archiviazione remoto non sia un server CA Enterprise Log Manager e che non sia necessario creare nuovi utenti, un gruppo e una struttura della directory che rispecchi quella di un server CA Enterprise Log Manager. Prima di inviare la chiave dal server di rapporto è necessario eseguire la procedura in quanto la comunicazione con il server di rapporto avviene mediante l'account caelmadmin creato dall'utente.

Per creare una struttura di file e impostare la proprietà del file sul server di archiviazione remoto

1. Accedere al server di archiviazione remoto, RSS, attraverso ssh come utente root.
2. Creare un nuovo utente chiamato caelmadmin.
3. Creare un gruppo chiamato caelmservice e creare un nuovo utente chiamato caelmservice.

4. Creare la directory da utilizzare come percorso remoto, che per impostazione predefinita è /opt/CA/LogManager.

   Nota: per utilizzare una directory diversa, specificare tale directory quando viene configurato il percorso remoto per l'archiviazione automatica.

5. Cambiare la directory principale per caelmservice in /opt/CA/LogManager o nella directory del percorso remoto. Il seguente esempio presuppone che la directory predefinita sia:

   ```
   usermod -d /opt/CA/LogManager caelmservice
   ```

6. Impostare le autorizzazioni del file per caelmservice. Il seguente esempio presuppone che la directory del percorso remoto predefinita sia:

   ```
   chown -R caelmservice:caelmservice /opt/CA/LogManager
   ```

7. Passare alla directory /opt/CA/LogManager o al percorso remoto alternativo.

8. Creare la cartella .ssh.

9. Assegnare la proprietà della cartella .ssh all'utente e al gruppo caelmservice:

   ```
   chown caelmservice:caelmservice .ssh
   ```

10. Disconnettersi dal server di archiviazione remota.

Configurazione delle chiavi per la coppia di archiviazione rapporto/remoto

Dopo aver configurato e convalidato l'autenticazione non interattiva da ciascun server di raccolta al server di rapporto, è necessario configurare e convalidare l'autenticazione non interattiva dal server di rapporto al server di archiviazione remoto.

Per lo scenario di esempio, la configurazione inizia con la generazione di una nuova coppia di chiavi RSA sul server di rapporto, ELM-RPT, e la copia della chiave pubblica come authorized_keys nella directory /tmp del server di archiviazione remoto, RSS.

Per generare una coppia di chiavi RSA sul server di rapporto e copiarla sul server di archiviazione remoto

1. Accedere al server di rapporto come caelmadmin.
2. Commutare gli utenti su root.

3. Commutare gli utenti sull'account caelmservice.

   ```
   su – caelmservice
   ```

4. Generare la coppia di chiavi RSA utilizzando il seguente comando:

   ```
   ssh-keygen –t rsa
   ```

5. Premere Invio per accettare il valore predefinito per ognuno dei seguenti prompt:

   - Specificare il file in cui salvare la chiave (/opt/CA/LogManager/.ssh/id_rsa):
   - Immettere la passphrase oppure lasciare il campo vuoto:
   - Immettere nuovamente la stessa passphrase:

6. Passare alla directory /opt/CA/LogManager.

7. Modificare i permessi della directory .ssh con il seguente comando:

   ```
   chmod 755 .ssh
   ```

8. Passare alla cartella .ssh.

9. Copiare il file id_rsa.pub in RSS, il server di archiviazione remoto di destinazione, utilizzando il seguente comando:

   ```
   scp id_rsa.pub caelmadmin@RSS:/tmp/authorized_keys
   ```

   Verrà creato il file authorized_keys nella directory /tmp sul server di archiviazione remoto con il contenuto della chiave pubblica.

Impostazione della proprietà del file della chiave sul server di archiviazione remoto

È possibile impostare la proprietà del file della chiave e le autorizzazioni su un server di archiviazione remoto dopo aver generato una coppia di chiavi sul server di rapporto e copiare la chiave pubblica sul server di archiviazione remoto.

Per spostare il file della chiave pubblica nella posizione corretta sul server di archiviazione remoto e impostare la proprietà del file

1. Accedere al server di archiviazione remoto come caelmadmin.

2. Commutare gli utenti su root.

3. Modificare le directory in: /opt/CA/LogManager/.ssh.
4. Copiare il file authorized_keys dalla directory /tmp alla directory attuale .ssh:

   ```
   cp /tmp/authorized_keys .
   ```

5. Modificare la proprietà del file authorized_keys con il comando:

   ```
   chown caelmservice:caelmservice authorized_keys
   ```

6. Modificare le autorizzazioni sul file authorized_keys:

   ```
   chmod 755 authorized_keys
   ```

   L'autenticazione non interattiva è ora configurata tra un server di rapporto CA Enterprise Log Manager e l'host remoto utilizzato per l'archiviazione.

Convalida dell'autenticazione non interattiva tra i server di rapporto e i server di archiviazione

Confermare che l'autenticazione non interattiva sia impostata tra il server di rapporto e il server di archiviazione remoto. Per lo scenario di esempio, il server di archiviazione remota è denominato RSS.

Per convalidare l'autenticazione non interattiva tra il server di rapporto CA Enterprise Log Manager e il server di archiviazione

1. Accedere al server di rapporto come root.
2. Passare gli utenti a caelmservice.

   ```
   su – caelmservice
   ```

3. Inserire il comando riportato di seguito:

   ```
   ssh caelmservice@RSS
   ```

   L'utente avrà accesso al server di archiviazione remoto senza immettere una passphrase.

Esempio: Configurazione dell'autenticazione non interattiva tra tre server

Lo scenario più semplice per la configurazione dell'autenticazione non interattiva, un prerequisito per l'archiviazione automatica, è uno scenario con due server CA Enterprise Log Manager, un server di raccolta e un server di rapporto/gestione, e un sistema di archiviazione remoto su un server UNIX o Linux. in questo esempio si presuppone che i tre server riservati all'archiviazione automatica siano denominati:

- Server di raccolta ELM NY
- Server di rapporto ELM NY
- Server di archiviazione NY

Le procedure per abilitare l'autenticazione non interattiva sono le seguenti:

1. Dal server di raccolta ELM NY, generare la coppia di chiavi RSA come caelmservice e copiare la chiave pubblica di questa coppia come authorized_keys nella directory /tmp sul server di rapporto ELM NY.
2. Creare una directory .ssh sul server di rapporto ELM NY, modificare la proprietà a caelmservice, spostare authorized_keys dalla directory /tmp alla directory .ssh e impostare la proprietà del file della chiave su caelmservice con le autorizzazioni necessarie.
3. Convalidare l'autenticazione non interattiva dal server di raccolta ELM NY al server di rapporto ELM NY.
4. Dal server di rapporto ELM NY, generare una coppia di chiavi RSA come caelmservice e copiare la chiave pubblica come authorized_keys nella directory /tmp del server di archiviazione ELM NY.
5. Dal server di archiviazione ELM NY, creare la struttura di directory /opt/CA/LogManager. Da questo percorso, creare una directory .ssh, modificare la proprietà a caelmservice, spostare authorized_keys alla directory .ssh e impostare la proprietà del file della chiave e delle autorizzazioni necessarie.
6. Convalidare l'autenticazione non interattiva dal server di rapporto ELM NY al server di archiviazione ELM NY.

I dettagli di questi passaggi sono simili a quelli dello scenario di hub e spoke. Per uno scenario di tre server, ignorare il passaggio 2 su coppie raccolta/rapporto aggiuntive e ignorare le istruzioni del passaggio 3 sulla concatenazione dei file in authorized_keys.

Esempio: archiviazione automatica fra tre server

Quando si utilizza la struttura raccolta-rapporto, occorre configurare l'archiviazione automatica dal server di raccolta al server di rapporto. Questa configurazione rende automatico il trasferimento di un database warm con dati del registro eventi raccolti e perfezionati al server di rapporto, dove è possibile creare i rapporti relativi. Si consiglia di pianificare la ricorrenza dell'archiviazione automatica perché si verifichi a ogni ora piuttosto che tutti i giorni, in modo da evitare di dedicare una grande quantità di tempo ogni giorno a un enorme trasferimento di dati. Scegliere una pianificazione basata sul proprio carico e decidere se sia meglio consolidare l'elaborazione o distribuirla nel corso della giornata. Quando i database vengono copiati tramite l'archiviazione automatica da un server di raccolta al relativo server di rapporto, tali database vengono eliminati dal server di raccolta.

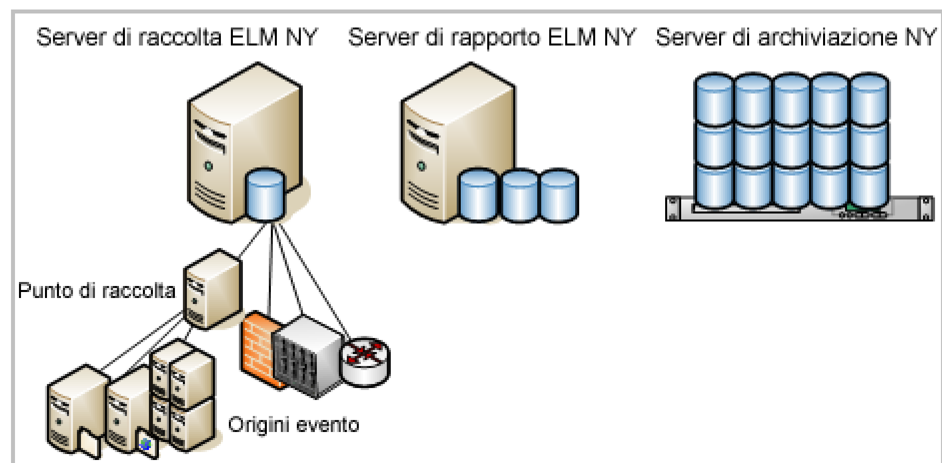
Dopo aver identificato un server locale con molto spazio di archiviazione, è possibile configurare l'archiviazione automatica dal server di rapporto a questo server di archiviazione remota. Quando i database vengono copiati tramite archiviazione automatica da un server di rapporto a un server di archiviazione remota, tali database rimangono intatti sul server di rapporto fino al momento in cui la configurazione relativa al numero massimo di giorni di archiviazione viene superata. A quel punto, i database vengono eliminati. Il vantaggio di questa fase di archiviazione automatica è quello di proteggere i database archiviati dalla perdita di dati dovuta al fatto di non essere stati trasferiti a una posizione per l'archiviazione a lungo termine prima dell'eliminazione automatica.

Nota: prima di configurare un server remoto perché riceva i database archiviati automaticamente, occorre impostare una struttura di directory su questo server di destinazione uguale a quella sul server CA Enterprise Log Manager di origine e assegnare le varie proprietà e le autorizzazioni per l'autenticazione. Per ulteriori informazioni, consultare "Configurazione dell'autenticazione non interattiva" nella *Guida all'implementazione*. Assicurarsi di seguire le istruzioni descritte in "Impostazione della proprietà di un file chiave su un host remoto".

In questo scenario di esempio, immaginare di essere un amministratore CA Enterprise Log Manager del centro dati di New York, che dispone di una rete di server CA Enterprise Log Manager, ognuno con un ruolo dedicato, più un server remoto con un'elevata capacità di archiviazione. Ecco i nomi dei server utilizzati per l'archiviazione automatica:

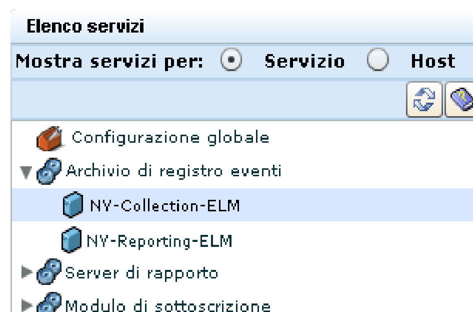
- Server di raccolta ELM NY
- Server di rapporto ELM NY
- Server di archiviazione NY

Nota: l'esempio presuppone l'esistenza di un server di gestione dedicato alla gestione del sistema di server CA Enterprise Log Manager. Questo server non è illustrato in questa sezione perché non ha un ruolo diretto nell'archiviazione automatica.



Per configurare l'archiviazione automatica dal server di raccolta al server di rapporto e poi dal server di rapporto al server di archiviazione remota, utilizzare l'esempio seguente come guida:

1. Selezionare la scheda Amministrazione e la sottoscheda Raccolta registri.
2. Espandere la cartella Archivio registro eventi e selezionare un server di raccolta.



3. Specificare che l'archiviazione automatica ricorre a ogni ora e che la destinazione sia il server di rapporto. Inserire le credenziali di un utente CA Enterprise Log Manager con ruolo di amministratore. Se sono presenti criteri personalizzati, questo utente deve avere diritti di modifica per la risorsa Database, il che garantisce la capacità di eliminare i database archiviati.

Auto Archive
Attivato
Tipo backup: Incremental
Frequenza: Hourly
Ora di inizio (in formato 24 ore): 0
Utente EEM: Administrator1
Password EEM: ********
Server Remoto: NY-Reporting-ELM
Utente Remoto: caelmservice
Posizione remota: /opt/CA/LogManager
Server ELM remoto

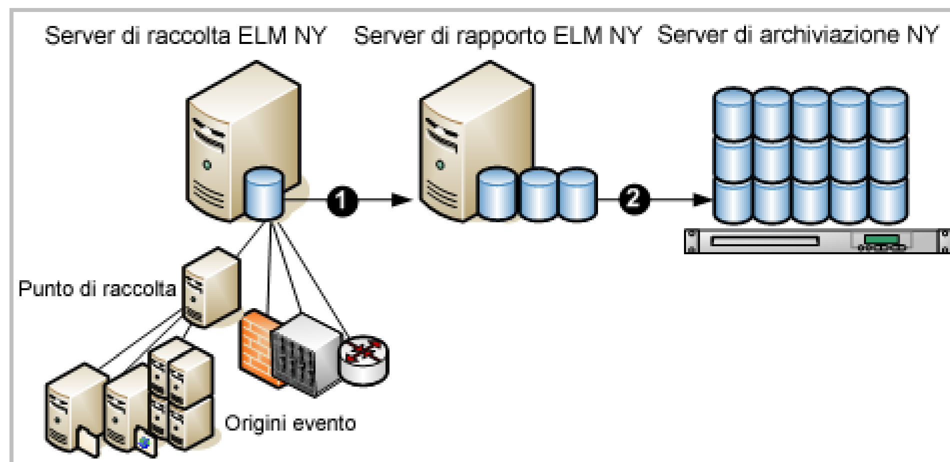
4. Selezionare il server di rapporto dall'Elenco servizi.

Elenco servizi
Mostra servizi per: Servizio Host
Configurazione globale
Archivio di registro eventi
NY-Collection-ELM
NY-Reporting-ELM
Server di rapporto
Modulo di sottoscrizione

5. Specificare l'archiviazione automatica giornaliera e come destinazione il server remoto utilizzato come archivio. Inserire le credenziali di un account utente con ruolo di amministratore. (Facoltativo) Creare un criterio di accesso a CALM con l'azione di modifica sulla risorsa database e assegnare un utente come identità. Inserire qui le credenziali di questo utente dai privilegi limitati.

Auto Archive
Attivato
Tipo backup: Incremental
Frequenza: Daily
Ora di inizio (in formato 24 ore): 1
Utente EEM: Administrator1
Password EEM: ********
Server Remoto: NY-Storage-Svr
Utente Remoto: caelmservice
Posizione remota: /opt/CA/LogManager
Server ELM remoto

I numeri sul diagramma seguente illustrano due configurazioni di archiviazione automatica: una dal server di raccolta al server di rapporto e l'altra dal server di rapporto a un server remoto sulla rete.



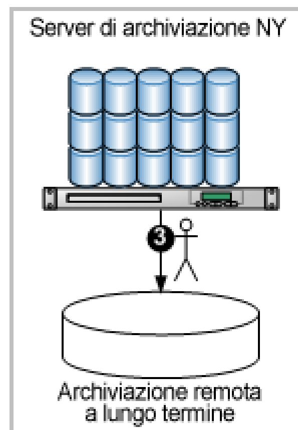
Una volta eseguita questa configurazione, l'elaborazione automatica funziona nel modo seguente:

1. Il server di raccolta ELM NY, ovvero il server di raccolta CA Enterprise Log Manager, raccoglie e perfeziona gli eventi e li inserisce nel database hot. Quando il database hot raggiunge il numero di record specificato, viene compresso in un database warm. Dato che la pianificazione stabilisce che l'archiviazione automatica venga eseguita una volta all'ora, a ogni ora il sistema copia i database warm e li trasferisce sul server di rapporto ELM NY, ovvero il server di rapporto CA Enterprise Log Manager. I database warm vengono eliminati dal server di raccolta ELM NY al momento del trasferimento.

2. Il server di rapporto ELM NY memorizza i database che possono essere interrogati fino a quando raggiungono la data specificata per Numero massimo di giorni di archiviazione, trascorsa la quale vengono eliminati. Dato che la pianificazione stabilisce che l'archiviazione automatica venga eseguita giornalmente, ogni giorno il sistema copia i database warm e li trasferisce sotto forma di database cold al server di archiviazione NY. I database cold possono rimanere sul server di archiviazione remota per un vasto periodo di tempo.

3. I database cold archiviati sul server di archiviazione NY della rete vengono trasferiti su una soluzione di archiviazione remota a lungo termine, dove possono restare per il numero di anni prestabilito.

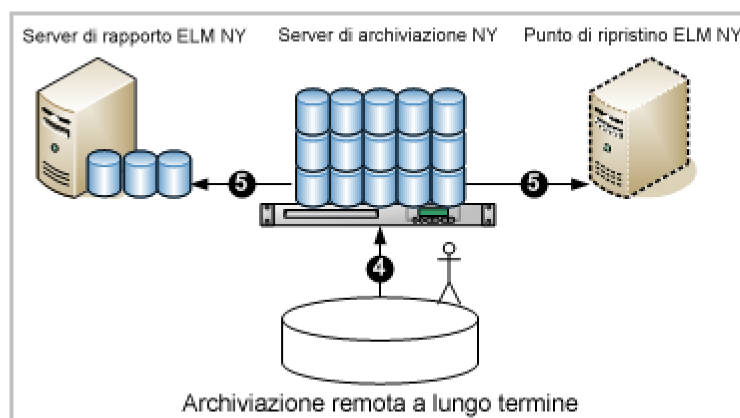
   Lo scopo dell'archiviazione è quello di conservare i registri eventi per il ripristino. I database cold possono essere ripristinati se si presenta l'esigenza di analizzare eventi datati che sono stati registrati. Il passaggio manuale del trasferimento dei database archiviati dal server di archiviazione on-site ad un archivio remoto a lungo termine viene illustrato nel diagramma seguente.



4. Si supponga che si verifichi una situazione che renda necessario esaminare i registri sottoposti a backup e trasferiti in una posizione remota. Per identificare il nome del database archiviato da ripristinare, cercare nel catalogo dell'archivio locale sul server di rapporto ELM NY (fare clic sulla scheda Amministrazione, selezionare Archivia query di catalogo dall'Explorer raccolta registri e fare clic su Query).

5. Recuperare il database archiviato identificato dall'archivio remoto. Copiarlo nuovamente nella directory /opt/CA/LogManager/data/archive sul server di archiviazione NY. Quindi, modificare la proprietà della directory di archiviazione in utente caelmservice.

6. Ripristinare come segue il database sul server di rapporto di origine o su un punto di ripristino dedicato all'analisi dei registri provenienti da database ripristinati:
   - Se si sta eseguendo il ripristino sul server di rapporto ELM NY, avviare lo script restore-ca-elm.sh dal server di rapporto ELM NY specificando come host remoto Server di archiviazione NY.
   - Se si sta eseguendo il ripristino sul punto di ripristino ELM NY, avviare lo script restore-ca-elm.sh dal punto di ripristino ELM NY specificando come host remoto Server di archiviazione NY.



Nota: ora è possibile eseguire query e rapporti sui dati ripristinati.

Ulteriori informazioni:

Informazioni sull'archiviazione automatica (a pagina 159)
Informazioni sui file di archivio (a pagina 158)
Impostazioni archivio registro eventi nell'ambiente di base (a pagina 178)
Esempio: mappa federazione di una grande impresa (a pagina 38)

Impostazioni archivio registro eventi nell'ambiente di base

In un ambiente in cui server CA Enterprise Log Manager distinti eseguono i ruoli di server di raccolta e di rapporto, è necessario configurare i depositi eventi di log singolarmente come configurazioni locali. Se si sceglie di utilizzare il server di rapporto per la gestione del traffico di failover, è possibile impostare un valore del campo Numero massimo di righe superiore rispetto al valore visualizzato nella tabella. Se si utilizza un server di gestione come server di rapporto, è possibile che il server di gestione generi informazioni evento sotto forma di eventi di automonitoraggio.

Nota: è necessario configurare ogni coppia di server che partecipa all'archiviazione automatica per l'autenticazione non interattiva per il funzionamento corretto della configurazione di archiviazione automatica.

La seguente tabella di esempio vengono illustrate alcune impostazioni di base. Il server CA Enterprise Log Manager di raccolta è nominato CollSrvr-1. Il server CA Enterprise Log Manager dei rapporti è nominato RptSrvr-1. Ad esempio, esiste un server di archiviazione remoto chiamato RemoteStore-1 per archiviare i file dei database cold e i file cold posizionati nella directory /CA-ELM_cold_storage.

Archivio registro eventi campo	Server di raccolta valori	Valori del server di rapporto
Numero massimo di righe	2000000 (predefinito)	Non valido per l'archiviazione automatica.
Giorni di archiviazione massimi	1 (Non valido per l'archiviazione automatica).	30 (Valido per l'archiviazione automatica e quando essa non è configurata).
Spazio su disco di archiviazione	10	10
Criterio di esportazione	24	72
Porta servizio sicuro	17001	17001
Opzioni archiviazione automatica		
Abilitato	Sì	Sì
Tipo backup	Incrementale	Incrementale
Frequenza	Ogni ora	Ogni giorno
Ora di inizio	0	23
Utente EEM	<CA Enterprise Log Manager_Administrator>	<CA Enterprise Log Manager_Administrator>
Password EEM	*<password>*	*<password>*
Server remoto	RptSrvr-1	RemoteStore-1
Utente remoto	caelmservice	user_X
Posizione remota	/opt/CA/LogManager	/CA-ELM_cold_storage
Server CA-ELM remoto	Sì	No

Le opzioni di archiviazione automatica riportate in questo esempio consentono di spostare i file di archivio (file di database warm) dal server di raccolta al server di rapporto ogni ora. Questo mantiene spazio su disco disponibile per gli eventi in ingresso. Entrambi i server utilizzano un backup incrementale per evitare di dover spostare grandi volumi di dati in una sola volta. In seguito al trasferimento di un database warm su un server di rapporto, il database verrà eliminato automaticamente dal server di raccolta.

Nota: il valore 0 dell'Ora di avvio non ha effetto quando la Frequenza del backup è impostata su Ogni ora.

Per l'utente EEM e la password EEM, specificare le credenziali di un utente CA Enterprise Log Manager assegnato al ruolo predefinito di amministratore o di un ruolo personalizzato associato a un criterio personalizzato che garantisce la possibilità di eseguire l'azione di modifica sulla risorsa del database.

Per il server di rapporto, specificare/opt/CA/LogManager come Posizione remota e caelmservice, come Utente remoto, in caso di archiviazione automatica dal server di rapporto al server di archiviazione remoto. Si creano questo percorso e questo utente quando si configura l'autenticazione non interattiva tra questi server.

Le opzioni di archiviazione automatica riportate in questo esempio consentono di spostare i file di archivio del server di report al server di archiviazione remota ogni giorno a partire dalle 23.00. In seguito al trasferimento di un database all'archiviazione cold sul server remoto, il database viene conservato sul server di rapporto durante un Numero massimo di giorni di archiviazione.

Se l'archiviazione automatica non è abilitata, i database warm vengono conservati in base alle soglie configurate per il Numero massimo di giorni di archiviazione e lo Spazio di archiviazione su disco, a seconda di quale si verifica prima. I database archiviati vengono conservati nel server di rapporto durante un periodo di 30 giorni prima di essere eliminati nel caso lo spazio su disco fosse inferiore al 10%. In questo caso, il server di rapporto genera un evento di automonitoraggio ed elimina i database più datati fino a quando lo spazio su disco disponibile è superiore al 10%. È possibile creare un avviso per notificare quando questo avviene attraverso e-mail o Feed RSS.

Quando un database viene ripristinato da un server di archiviazione remoto al server di rapporto originale, viene conservato durante un periodo di 3 giorni (72 ore).

Ulteriori informazioni su ognuno di questi campi e sui rispettivi valori sono disponibili nella guida online.

Impostazione delle opzioni dell'archivio registro eventi

La finestra della configurazione dell'archivio registro eventi permette di impostare le opzioni globali di tutti i server CA Enterprise Log Manager. È inoltre possibile fare clic sulla freccia accanto alla voce per espandere il nodo dell'archivio registro eventi. Questa operazione consente di visualizzare i singoli server CA Enterprise Log Manager presenti nella rete. Facendo clic su tali nomi di server sarà possibile impostare le opzioni di configurazione locali specifiche di ogni server, se lo si desidera.

Gli utenti con ruolo di amministratore possono configurare qualsiasi server CA Enterprise Log Manager da qualsiasi altro server CA Enterprise Log Manager.

Per impostare le opzioni dell'archivio registro eventi

1. Accedere al server CA Enterprise Log Manager e selezionare la scheda Amministrazione.

   La sottoscheda Raccolta registri verrà visualizzata per impostazione predefinita.

2. Fare clic sulla sottoscheda Servizi.

3. Selezionare la voce Archivio registro eventi.

   Le opzioni predefinite forniscono una buona configurazione iniziale per una rete di medie dimensioni con velocità moderata.

   Informazioni aggiuntive su ogni campo sono disponibili nella Guida in linea.

   Nota: le tabelle Figlio della federazione e Archiviazione automatica appaiono solo quando vengono visualizzate le opzioni locali di un singolo server CA Enterprise Log Manager.

Considerazioni su ODBC Server

È possibile installare un client ODBC o JDBC per accedere al deposito eventi di log di CA Enterprise Log Manager da un'applicazione esterna come SAP BusinessObjects Crystal Reports.

Da questa area di configurazione è possibile eseguire le seguenti attività:

- Abilitare o disabilitare l'accesso di ODBC e di JDBC al deposito eventi di log.
- Impostare la porta di servizio utilizzata per le comunicazioni fra il client ODBC o JDBC ed il server CA Enterprise Log Manager
- Specificare se le comunicazioni fra il client ODBC o JDBC e CA Enterprise Log Manager sono crittografate.

Le descrizioni dei campi sono le seguenti:

Abilita servizio

Indica se i client ODBC o JDBC possono accedere ai dati nel deposito eventi di log. Selezionare questa casella di controllo per abilitare l'accesso esterno agli eventi. Deselezionare la casella di controllo per disabilitare l'accesso esterno.

Il servizio ODBC non è attualmente compatibile con FIPS. Deselezionare questa casella di controllo per prevenire l'accesso di ODBC e JDBC in caso di esecuzione in modalità FIPS. In questo modo viene evitato l'accesso non conforme ai dati evento. Se si desidera disabilitare i servizi ODBC e JDBC per eseguire operazioni in modalità FIPS, assicurarsi di impostare questo valore per *ogni* server di una federazione.

Porta di ascolto del server

Specifica il numero di porta utilizzato dai servizi ODBC o JDBC. Il valore predefinito è 17002. Il server CA Enterprise Log Manager rifiuta i tentativi di connessione quando è specificato un valore diverso nella stringa di origine dati di Windows o dell'URL JDBC.

Crittografato (SSL)

Indica se utilizzare la crittografia per le comunicazioni fra il client ODBC ed il server CA Enterprise Log Manager. Il server CA Enterprise Log Manager rifiuta i tentativi di connessione quando il valore in origine dati di Windows o nell'URL JDBC non corrisponde a questa impostazione.

Timeout di sessione (minuti)

Specifica il numero di minuti in cui una sessione inattiva resterà aperta prima che si chiuda automaticamente.

Livello di log

Definisce il tipo e il livello di dettaglio presenti nel file in registrazione. L'elenco a discesa è disposto in ordine di dettaglio: la prima voce corrisponde alla meno dettagliata.

Applica a tutti i registratori

Controlla se l'impostazione del livello di log sovrascrive tutte le impostazioni di log dal file delle proprietà del log. Questa impostazione si applica soltanto quando l'impostazione del livello di log è inferiore (ovvero più dettagliata) rispetto a quella predefinita.

Considerazioni sul server di rapporto

Il server di rapporto controlla l'amministrazione dei rapporti distribuiti automaticamente, il relativo aspetto in formato PDF e la conservazione di rapporti e avvisi. Dall'area di configurazione del server è possibile eseguire le seguenti attività:

- Creare elenchi definiti dall'utente:

  Elenchi definiti dall'utente (valori chiave)

  Consente di creare gruppi di rilevanza da utilizzare nella creazione di rapporti e di controllare i periodi di tempo cui si applicano.

- Nell'area Impostazioni di posta elettronica, impostare il server di posta, l'indirizzo di posta elettronica dell'amministratore, la porta SMTP e le informazioni di autenticazione.
- Nell'area Configurazioni rapporto, controllare il nome ed il logo della società, i caratteri e le altre impostazioni dei rapporti PDF.
- Nell'area Memorizzazione avvisi, impostare il totale degli avvisi memorizzati ed il numero di giorni in cui saranno conservati:

  Numero massimo di avvisi

  Definisce il numero massimo di avvisi conservati dal server di rapporto per la consultazione.

  Minimo: 50

  Massimo: 1000

  Memorizzazione avvisi

  Definisce il numero di giorni in cui gli avvisi vengono conservati, fino al numero massimo possibile.

  Minimo: 1

  Massimo: 30

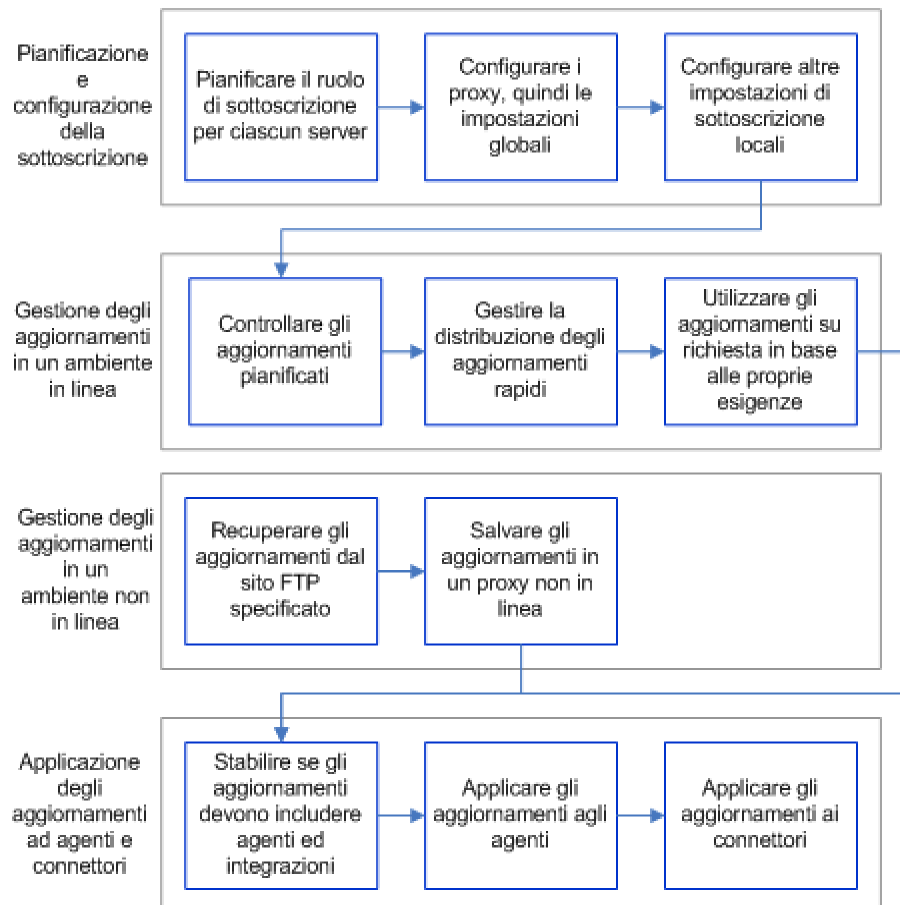
- Impostare, nell'area Memorizzazione rapporti, i criteri di memorizzazione per ogni tipo di ricorrenza dei rapporti pianificati.

- Impostare la frequenza con cui l'utilità di memorizzazione ricercherà i rapporti da eliminare automaticamente in base a tali criteri. Ad esempio, se l'utilità di memorizzazione dei rapporti viene eseguita giornalmente, verranno eliminati ogni giorno i rapporti con un'età superiore a quella massima specificata.
- Definire le impostazioni dei processi CA IT PAM
- Regolare le impostazioni dei trap SNMP

Diagramma di flusso della distribuzione delle sottoscrizioni

è possibile gestire gli aggiornamenti per l'applicazione CA Enterprise Log Manager, gli aggiornamenti di agenti e connettori e gli aggiornamenti del contenuto tramite la funzionalità di sottoscrizione. Il seguente diagramma di flusso fa riferimento a pianificazione, configurazione, gestione degli aggiornamenti in un ambiente in linea e non in linea e all'applicazione di aggiornamenti di agenti e connettori. La pianificazione e la configurazione sono inclusi in questa guida.

Nota: per ulteriori informazioni sull'utilizzo degli aggiornamenti su richiesta, la gestione degli aggiornamenti in un ambiente non in linea e l'applicazione di aggiornamenti di agenti e connettori, consultare la *Guida all'amministrazione*.



Configurazione della sottoscrizione

Il Modulo di sottoscrizione è simile ad altri servizi per il fatto che sono entrambi sia impostazioni globali che locali.

Il Modulo di sottoscrizione si distingue da altri servizi per quanto segue:

- Le impostazioni globali che richiedono la selezione di proxy dipendono da impostazioni eseguite a livello locale. Si impostano i proxy di sottoscrizione per gli aggiornamenti del contenuto a livello globale, ma l'elenco disponibile dei proxy non viene popolato fino a quando i proxy sono configurati. Si configurano i server che devono operare come proxy a livello locale, sia come proxy che come proxy non in linea.
- Non tutti i server CA Enterprise Log Manager locali non sono simili in termini di esigenze di configurazione. Server diversi hanno ruoli diversi. Il ruolo del server stabilisce quali impostazioni devono essere configurate.

Le impostazioni di sottoscrizione globali variano nell'applicabilità, come segue:

- Di seguito sono indicate le impostazioni che non possono essere ignorate a livello locale (solo globali):
  - Proxy di sottoscrizione predefinito
  - URL Feed RSS: utilizzato da tutti i proxy online
  - Chiave pubblica: utilizzata da tutti i proxy online

    Importante: Non aggiornare manualmente queste impostazioni.
  - Cancella aggiornamenti che risalgono a più di n giorni: vale per tutti i proxy (online e non in linea)
  - Riavvio automatico dopo l'aggiornamento del sistema operativo: vale per tutti i client

    Nota: tutti i CA Enterprise Log Manager sono client, inclusi i server proxy o proxy non in linea.
  - Proxy di sottoscrizione per l'aggiornamento dei contenuti
- Impostazioni configurate solo a livello locale
  - Proxy di sottoscrizione
  - Proxy di sottoscrizione non in linea

Tra le impostazioni globali che possono essere ignorate a livello locale, la possibilità di ignorare dipende dal fatto che il server sia definito come proxy in linea o client. Seguono dettagli:

- Impostazioni valide per i proxy online che è possibile ignorare
  - Cinque impostazioni relative a proxy HTTP
  - Moduli da aggiornare
- Impostazioni valide per i client di sottoscrizione che è possibile ignorare
  - Proxy di sottoscrizione per il client

Configurazione impostazioni sottoscrizione globale

È possibile configurare le impostazioni della sottoscrizione globale non appena sono stati installati tutti i server CA Enterprise Log Manager.

Considerare la configurazione delle impostazioni proxy per i server che si intende assegnare come proxy di sottoscrizione (online o non in linea) prima di configurare le impostazioni di sottoscrizione globale. Questa impostazione popola gli elenchi disponibili globali dei proxy per i client e dei proxy per gli aggiornamenti dei contenuti.

Per configurare le impostazioni di sottoscrizione globale

1. Fare clic sulla scheda Amministrazione, selezionare Servizi, fare clic sul Modulo di sottoscrizione ed esaminare la configurazione dei servizi globali: impostazioni Modulo di sottoscrizione nel riquadro a destra.
2. Accettare o modificare le impostazioni del proxy di sottoscrizione predefinito. Il *proxy di sottoscrizione predefinito* di solito è il server CA Enterprise Log Manager che viene installato per primo e può essere anche il server CA Enterprise Log Manager di gestione. Questo è il server che verrà contattato da ogni client di sottoscrizione in linea per cui non è stato configurato un elenco di proxy di sottoscrizione. Se tale elenco dei proxy di sottoscrizione esiste, ma è esaurito durante la ricerca, il client riceverà gli aggiornamenti da questo predefinito.

   Nota: questa impostazione non può essere ignorata a livello locale. Ciò che viene specificato qui vale per tutti i server CA Enterprise Log Manager che utilizzano lo stesso server CA Enterprise Log Manager di gestione.

3. Impostare la pianificazione per il proxy predefinito e per i proxy online per contattare il server di sottoscrizione CA per gli aggiornamenti. I client contattano i proxy per gli aggiornamenti dopo che il proxy ha scaricato l'aggiornamento dal server di sottoscrizione di CA.

   a. Specificare in ore la frequenza con cui il proxy deve contattare il server di sottoscrizione CA per gli aggiornamenti nel campo Frequenza aggiornamento.

   b. Utilizzare le seguenti linee guida per l'impostazione dell'Ora di inizio aggiornamento.

      - Se si specifica un valore inferiore a 24 per la Frequenza aggiornamento, non effettuare selezioni con la casella di selezione Ora di inizio aggiornamento. Gli aggiornamenti della sottoscrizione iniziano quando viene avviato iGateway.

      - Se si specifica un valore pari o superiore a 24 per la Frequenza aggiornamento, specificare su un orologio a 24 ore l'ora di inizio dell'aggiornamento.

4. Accettare l'URL del Feed RSS, che collega al server di sottoscrizione CA. Questo URL permette di popolare i moduli disponibili da scaricare.

5. Accettare la chiave pubblica visualizzata o selezionare la versione corretta. Poiché questa chiave è utilizzata da tutti i proxy di sottoscrizione, non può essere modificata a livello del server locale.

   Importante: Non modificare questi valori, a meno che l'operazione non avvenga sotto il diretto controllo del personale dell'assistenza tecnica. Quando è necessario sostituire la chiave per un determinato download, questo campo viene aggiornato automaticamente prima dell'inizio del download.

6. Specificare un valore in giorni o accettare quello predefinito, 30, per la durata della conservazione degli aggiornamenti scaricati all'interno del sistema. Concedere una durata di tempo sufficiente per copiare la directory dei download da un proxy di sottoscrizione di origine a tutti i proxy di sottoscrizione non in linea e affinché tutti gli aggiornamenti vengano scaricati e installati da tutti i client.

   Nota: l'impostazione di cancellazione degli aggiornamenti vale per tutti i proxy di sottoscrizione e i proxy di sottoscrizione non in linea e non può essere modificata a livello locale.

7. Considerare quanto segue durante la configurazione del Riavvio automatico dopo l'aggiornamento del sistema operativo, che vale per tutti i CA Enterprise Log Manager, quando viene scaricato e installato un aggiornamento del sistema operativo:
   - Accettare l'impostazione predefinita, No, per specificare nessun riavvio automatico del server CA Enterprise Log Manager se l'aggiornamento dei file binari include l'installazione di patch al sistema operativo che richiedono il riavvio del server per il completamento dell'aggiornamento. Quando si imposta No, gli utenti riceveranno la notifica con un evento di automonitoraggio per riavviare manualmente il sistema.
   - Specificare Sì per assicurare che il server CA Enterprise Log Manager venga spento e riavviato automaticamente dopo ogni installazione di patch del sistema operativo che richiedono un riavvio completo.
8. Selezionare tra i moduli da scaricare disponibili quelli adatti al sistema operativo. Ad esempio, se non sono disponibili server CA Enterprise Log Manager che utilizzano una determinata applicazione o sistema operativo, non si deve selezionare il modulo da scaricare.

   Nota: l'elenco disponibile è popolato al ciclo di aggiornamento successivo all'immissione di un URL di feed RSS valido. Quando questo avviene è stabilito dall'ora di inizio aggiornamento specificata e dalla frequenza di aggiornamento specificata. Se l'URL del feed RSS è impostato e i Moduli da scaricare non sono popolati, assicurarsi che l'URL sia valido. Se la rete si trova dietro a un firewall, assicurarsi che l'impostazione del proxy HTTP sia attiva e che le impostazioni associate siano corrette per il proxy di sottoscrizione in linea.
9. Dall'elenco "Proxy di sottoscrizione disponibili per il client" selezionare uno o più proxy, che verranno contattati dai client in modalità round robin per ricevere aggiornamenti del sistema operativo e del software CA Enterprise Log Manager. Per una grande azienda, questa impostazione deve essere modificata a livello locale. Considerare di fornire l'elenco che verrà utilizzato dalla maggior parte dei client o un "superelenco" che include quali configurazioni locali i proxy possono scegliere.

   Nota: questa impostazione può essere utilizzata anche per creare un'architettura proxy a livelli, in cui un proxy di sottoscrizione contatta i proxy di sottoscrizione selezionati affinché gli aggiornamenti vengano trasferiti ai client, anziché contattare direttamente il server di sottoscrizione CA.

10. Dall'elenco "Proxy di sottoscrizione disponibili per gli aggiornamenti di contenuto" selezionare il proxy che deve inviare gli aggiornamenti non binari all'archivio utente CA Enterprise Log Manager. È consigliabile selezionare un secondo proxy come riserva per garantire la distribuzione degli aggiornamenti se il server che esegue normalmente tale operazione non dovesse essere disponibile. Gli aggiornamenti non binari includono file XMP, file DM, integrazioni, aggiornamenti di configurazione per moduli CA Enterprise Log Manager e aggiornamenti di chiavi pubbliche. In un ambiente non in linea, è possibile selezionare il proxy non in linea che invia gli aggiornamenti all'archivio utente di CA Enterprise Log Manager.
11. Se la rete si trova dietro a un firewall ed è disponibile un server proxy HTTP, modificare l'impostazione in Sì e completare i quattro campi relativi. Fare clic su Verifica proxy per verificare la connettività. Queste impostazioni possono essere ignorate da server configurati come proxy di sottoscrizione in linea.
12. Fare clic su Salva.

Ulteriori informazioni:

Considerazioni sulla sottoscrizione (a pagina 190)
Valutazione della necessità di un proxy HTTP (a pagina 54)
Verifica dell'accesso a Feed RSS per la sottoscrizione (a pagina 55)
Componenti e porte di sottoscrizione (a pagina 52)

Considerazioni sulla sottoscrizione

Un sistema di server proxy/client eroga aggiornamenti. Il primo server installato viene impostato come server proxy di sottoscrizione predefinito; esso contatta periodicamente il server di sottoscrizione CA alla ricerca di aggiornamenti. Le successive installazioni verranno configurate come client di tale server proxy, il quale verrà contattato per gli aggiornamenti.

Il sistema predefinito consente di ridurre il traffico di rete eliminando la necessità per ogni server di contattare il server di sottoscrizione CA in modo diretto, essendo tuttavia completamente configurabile. Se necessario, è possibile aggiungere server proxy.

Inoltre, è possibile ridurre ulteriormente il traffico Internet creando server proxy non in linea, che consentono di memorizzare localmente le informazioni di aggiornamento e di inviarle ai client contattati. È possibile supportare eventuali server proxy non in linea, copiando manualmente nel percorso di download del proxy non in linea quanto presente nel percorso del proxy in linea. I proxy non in linea devono essere configurati in ambienti in cui sono presenti server CA Enterprise Log Manager che non possono accedere a Internet o a un server connesso a Internet.

Nel configurare il servizio di sottoscrizione, tenere presenti le seguenti informazioni su alcune impostazioni e le relative interazioni:

Proxy di sottoscrizione predefinito

Definisce il server proxy predefinito per il servizio di sottoscrizione. Questo proxy deve disporre di accesso a Internet. Se non si definiscono altri proxy di sottoscrizione, tale server otterrà gli aggiornamenti di sottoscrizione dal server di sottoscrizione CA e scaricherà gli aggiornamenti binari su tutti i client per poi distribuire gli aggiornamenti di contenuto. Se si definiscono altri proxy, i client contatteranno questo server per gli aggiornamenti nel caso in cui non sia configurato alcun elenco di proxy di sottoscrizione oppure quando l'elenco configurato sarà esaurito. Il valore predefinito è il primo server installato nel proprio ambiente. Tale valore è disponibile soltanto come impostazione globale.

Proxy di sottoscrizione

Controlla se il server locale è un proxy di sottoscrizione. Un proxy di sottoscrizione in linea utilizza l'accesso a Internet per ottenere aggiornamenti di sottoscrizione dal relativo server CA. È possibile configurare i proxy di sottoscrizione in linea in modo da scaricare gli aggiornamenti binari sui client ed inviare gli aggiornamenti di contenuto al server di gestione. È anche possibile utilizzare un proxy in linea come origine per copiare gli aggiornamenti sui proxy di sottoscrizione non in linea. Se selezionata, la casella di controllo Proxy di sottoscrizione non in linea deve essere deselezionata. Tale valore è disponibile soltanto come impostazione locale.

Nota: deselezionando entrambe le caselle di controllo relative ai proxy di sottoscrizione, il server diventerà un client di sottoscrizione.

Proxy di sottoscrizione non in linea

Controlla se il server locale è un proxy di sottoscrizione non in linea. Un proxy di sottoscrizione non in linea è un server che ottiene aggiornamenti di sottoscrizione tramite una copia della directory manuale (usando scp) da un proxy di sottoscrizione online. È possibile configurare i proxy di sottoscrizione non in linea per scaricare gli aggiornamenti binari nei client. I proxy di sottoscrizione non in linea non richiedono un accesso ad Internet. Se selezionata, la casella di controllo Proxy di sottoscrizione deve essere deselezionata. Tale valore è disponibile soltanto come impostazione locale.

Nota: deselezionando entrambe le caselle di controllo dei proxy di sottoscrizione, il server diventerà un client di sottoscrizione.

Ora di inizio aggiornamento

Vale solo quando la frequenza di aggiornamento è pari o superiore a 24.

Definisce l'ora di inizio del primo controllo di aggiornamento (in ore intere) in base all'ora locale del server. Il valore è un orologio di 24 ore. Tale valore si applica al controllo dell'aggiornamento iniziale. La frequenza di aggiornamento consente di controllare le tempistiche dei controlli di aggiornamento successivi. Questa impostazione si applica soltanto al server proxy di sottoscrizione.

Limiti: 0-23, dove 0 indica la mezzanotte e 23 le 11.00 di sera.

Frequenza di aggiornamento

Definisce la frequenza in ore con la quale il proxy in linea contatta il server di sottoscrizione CA e la frequenza con cui il client di sottoscrizione contatta il proxy. Questa impostazione si applica soltanto al server proxy di sottoscrizione.

Esempi: .5 significa ogni 30 minuti, 48 significa a giorni alterni.

Aggiorna ora

Fare clic su questo pulsante per avviare immediatamente un ciclo di aggiornamento su richiesta per il server selezionato. È possibile eseguire un aggiornamento su richiesta solo per un server alla volta. Aggiornare il server proxy di sottoscrizione prima di eseguire tale operazione su un client dello stesso tipo.

URL del feed RSS

Definisce l'URL del server di sottoscrizione CA. I proxy di sottoscrizione in linea utilizzano questo URL per accedere al server di sottoscrizione CA e scaricare gli aggiornamenti relativi. Tale valore è disponibile soltanto come impostazione globale.

Server proxy HTTP

Controlla se questo server contatta il server di sottoscrizione CA per l'aggiornamento tramite un proxy HTTP, anziché in maniera diretta.

Indirizzo proxy da utilizzare

Consente di specificare l'indirizzo IP completo del proxy HTTP.

Porta

Specifica il numero della porta utilizzata per contattare il proxy HTTP.

ID utente proxy HTTP

Specifica l'ID utente utilizzato per contattare il proxy HTTP.

Password proxy HTTP

Specifica la password utilizzata per contattare il proxy HTTP.

Chiave pubblica

Definisce la chiave utilizzata per testare e verificare la firma degli aggiornamenti. Evitare di aggiornare manualmente questo valore. Aggiornando una coppia di chiavi pubblica-privata, il proxy scaricherà l'aggiornamento del valore della chiave pubblica, aggiornandola. Tale valore è disponibile soltanto come impostazione globale.

Cancella aggiornamenti che risalgono a più di

Definisce il numero di giorni per i quali il server proxy conserverà i pacchetti di aggiornamento. Tale valore è disponibile soltanto come impostazione globale.

Riavvio automatico dopo l'aggiornamento del sistema operativo

Controlla se si verifica il riavvio automatico di CA Enterprise Log Manager dopo un aggiornamento del sistema operativo. Tale valore è disponibile soltanto come impostazione globale.

Moduli da scaricare

Consente di selezionare i moduli applicabili al proprio ambiente operativo. I moduli selezionati per i proxy determinano i moduli scaricati dal server di sottoscrizione CA come parte degli aggiornamenti di sottoscrizione. I moduli selezionati per i client vengono utilizzati per aggiornare i moduli corrispondenti installati al loro interno. È possibile selezionare un modulo da scaricare per un client non selezionato per il proxy. Il proxy eseguirà il recupero del modulo per il client, senza installarlo su sé stesso.

Nota: se non è già presente, impostare l'URL del feed RSS. Tale impostazione consente al sistema di leggere il feed RSS e, nell'intervallo di aggiornamento successivo, di visualizzare l'elenco dei moduli disponibili per il download.

Proxy di sottoscrizione per il client

Consente di impostare i proxy contattati per gli aggiornamenti di prodotti e del sistema operativo da tutti i client o dal client selezionato. È possibile utilizzare le frecce verso l'alto e verso il basso per controllare l'ordine con cui il client contatta i proxy di sottoscrizione. Il client scaricherà gli aggiornamenti dal primo proxy raggiungibile. Se nessuno dei proxy configurati è disponibile, il client contatta il proxy di sottoscrizione predefinito.

Proxy di sottoscrizione per l'aggiornamento dei contenuti

Consente di selezionare i proxy da utilizzare per distribuire gli aggiornamenti dei contenuti all'archivio utente. È possibile selezionare proxy in linea o non in linea. Tale valore è disponibile soltanto come impostazione globale.

Nota: si consiglia di selezionare più di un client per questioni di ridondanza.

Configurazione di server CA Enterprise Log Manager per la sottoscrizione

Uno o più server CA Enterprise Log Manager sono elencati in Modulo di sottoscrizione. Ogni server eredita le impostazioni della sottoscrizione globale. Quando vengono visualizzate inizialmente, tutte le impostazioni sono disattivate. Per ignorare tutte le impostazioni, fare clic sul pulsante di attivazione globale/locale per modificare il campo.

Ogni server elencato deve essere configurato come uno dei seguenti:

- Proxy di sottoscrizione (online)
- Proxy di sottoscrizione non in linea
- Client di sottoscrizione

Proxy di sottoscrizione online e non in linea installano automaticamente gli aggiornamenti e agiscono come proprio client. Tutti i server CA Enterprise Log Manager che non sono proxy di sottoscrizione devono essere configurati come client.

Un proxy di sottoscrizione speciale è il proxy di sottoscrizione predefinito. Il primo server CA Enterprise Log Manager installato si registra con l'archivio utente CA Enterprise Log Manager come proxy di sottoscrizione predefinito, ma questa impostazione può essere modificata a livello globale. In un ambiente online, tutti i client scaricano aggiornamenti delle sottoscrizioni dal proxy di sottoscrizione predefinito se non sono configurati i proxy aggiuntivi o quando questi non sono disponibili.

Ulteriori informazioni:

Esempio: configurazione della sottoscrizione con sei server (a pagina 63)
Configurazione di un proxy di sottoscrizione in linea (a pagina 195)
Configurazione di un proxy di sottoscrizione non in linea (a pagina 197)

Configurazione di un proxy di sottoscrizione in linea

È possibile utilizzare il server predefinito come unico server di sottoscrizione in linea. In questo caso, tutti gli altri server CA Enterprise Log Manager competeranno per scaricare gli aggiornamenti delle sottoscrizioni da questo unico server. Questa configurazione è adatta a una piccola installazione, in cui proxy di sottoscrizione in linea non sono necessari.

Per una grande installazione, è buona prassi configurare server aggiuntivi. Quando diversi server vengono configurati come proxy di sottoscrizione in linea in un ambiente online, è possibile selezionare proxy che ogni client può interrogare. Quando un client può contattare server diversi in modo round robin, può scaricare più facilmente gli aggiornamenti della sottoscrizione in modo tempestivo.

Il percorso di download preconfigurato segue:
.../opt/CA/LogManager/data/subscription.

Solo gli amministratori possono configurare proxy di sottoscrizione.

Per configurare un proxy di sottoscrizione in linea

1. Fare clic sulla scheda Amministrazione, selezionare Servizi, espandere il Modulo di sottoscrizione e selezionare il server da configurare.

   Comparirà la Configurazione del servizio del modulo di sottoscrizione per il server CA Enterprise Log Manager selezionato.

2. Selezionare il proxy di sottoscrizione e lasciare l'opzione Non in linea disattivata.

   ☑ Proxy di sottoscrizione?

   ☐ Proxy di sottoscrizione non in linea?

3. Per ignorare un'impostazione globale, fare clic sul pulsante di attivazione globale/locale per passare alla configurazione servizio locale per il campo selezionato, quindi apportare le modifiche richieste.

   Nota: facendo clic nuovamente sul pulsante di attivazione per bloccare il campo e utilizzare l'impostazione globale, il valore viene modificato al valore globale all'intervallo di aggiornamento successivo, come stabilito nella configurazione globale.

4. Considerare l'accettazione delle impostazioni globali per Ora di inizio aggiornamento e Frequenza aggiornamento.

5. Se questo server deve scaricare gli aggiornamenti della sottoscrizione attraverso un server proxy HTTP diverso da quello ereditato, passare alla configurazione locale e modificare i cinque campi che configurano il proxy HTTP.

6. Se i moduli necessari per scaricare gli aggiornamenti del prodotto CA Enterprise Log Manager o del sistema operativo sono diversi dalle impostazioni ereditate, passare alla configurazione locale e apportare le modifiche necessarie.

7. Fare clic su Salva.

Ulteriori informazioni:

Considerazioni sulla sottoscrizione (a pagina 190)

Configurazione di un proxy di sottoscrizione non in linea

Quando i server CA Enterprise Log Manager non sono connessi a internet, è necessario configurare uno o più server CA Enterprise Log Manager come proxy di sottoscrizione non in linea da cui altri server client non in linea possono ricevere aggiornamenti delle sottoscrizioni.

Un amministratore deve copiare gli aggiornamenti delle sottoscrizioni da un proxy online ai proxy non in linea. Il percorso di download preconfigurato segue: .../opt/CA/LogManager/data/subscription.

Solo gli amministratori possono configurare proxy di sottoscrizione.

Per configurare un proxy di sottoscrizione non in linea

1. Fare clic sulla scheda Amministrazione, selezionare Servizi, espandere il Modulo di sottoscrizione e selezionare il server da configurare.

   Comparirà la Configurazione del servizio del modulo di sottoscrizione per il server CA Enterprise Log Manager selezionato.

2. Selezionare proxy di sottoscrizione non in linea.

   ☐ Proxy di sottoscrizione?

   ☑ Proxy di sottoscrizione non in linea?

3. Fare clic su Salva.

   Ora è possibile configurare questo proxy di sottoscrizione non in linea come segue:

   - Aggiungerlo all'impostazione globale per Proxy di sottoscrizione per l'aggiornamento dei contenuti
   - Aggiungerlo all'impostazione globale e/o alle impostazioni di ogni client locale per Proxy di sottoscrizione per il client

Ulteriori informazioni:

Valutazione della necessità di un proxy di sottoscrizione non in linea (a pagina 56)

Configurazione di un client di sottoscrizione

Tutti i server CA Enterprise Log Manager che non sono proxy di sottoscrizione sono configurati come client, per impostazione predefinita. Non è necessario configurare i client di sottoscrizione a meno che si voglia ignorare l'elenco dei proxy selezionato impostato globalmente.

Un client di sottoscrizione è un server CA Enterprise Log Manager in grado di ottenere aggiornamenti di contenuto da un altro server CA Enterprise Log Manager, denominato server proxy di sottoscrizione. I client di sottoscrizione sondano regolarmente i server proxy di sottoscrizione configurati, e prelevano i nuovi aggiornamenti quando sono disponibili. Dopo aver prelevato gli aggiornamenti, il client installa i componenti scaricati.

Per configurare un client di sottoscrizione

1. Fare clic sulla scheda Amministrazione, selezionare Servizi, espandere il Modulo di sottoscrizione e selezionare il server da configurare.

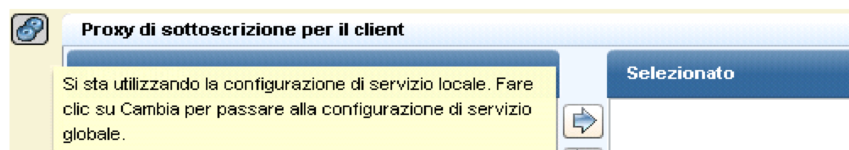
   Viene visualizzata la configurazione di servizio del modulo di sottoscrizione per il server CA Enterprise Log Manager selezionato.

2. Identificare il server selezionato come client deselezionando le caselle di controllo dei due proxy di sottoscrizione.

   ☐ Proxy di sottoscrizione?

   ☐ Proxy di sottoscrizione non in linea?

3. Fare clic sul pulsante di attivazione globale/locale per la configurazione del servizio locale di Proxy di sottoscrizione per il client e selezionare i proxy di sottoscrizione che questo client deve contattare, in modalità round-robin, per aggiornamenti dei prodotti e del sistema operativo.

4. Se i moduli necessari per scaricare gli aggiornamenti del prodotto o del sistema operativo sono diversi dalle impostazioni ereditate, passare alla configurazione locale e apportare le modifiche necessarie. È possibile scaricare moduli come client non selezionati dal proxy.

5. Fare clic su Salva.

Ulteriori informazioni:

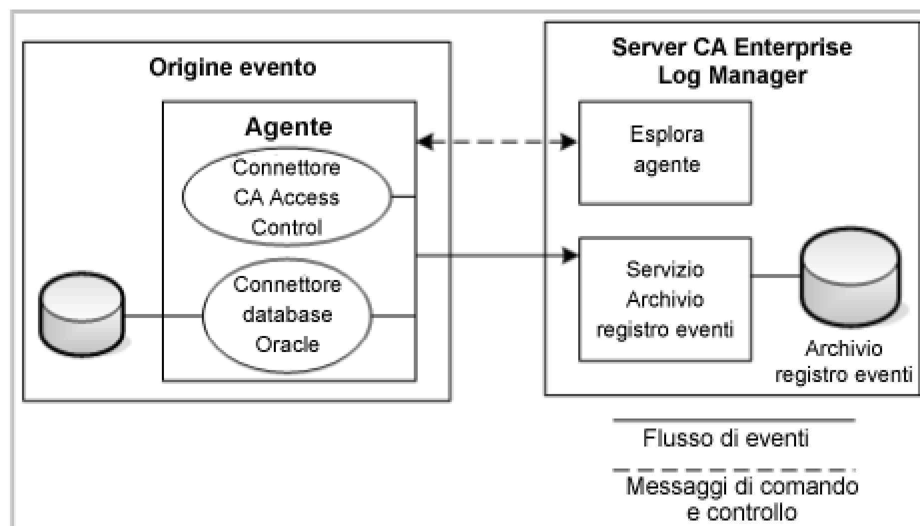
Valutazione della necessità di un elenco di proxy (a pagina 62)
Considerazioni sulla sottoscrizione (a pagina 190)

Capitolo 6: Configurazione della raccolta eventi

Questa sezione contiene i seguenti argomenti:

Installazione di agenti

Con installazioni separate per piattaforme specifiche, gli agenti CA Enterprise Log Manager forniscono il layer di trasporto per trasferire gli eventi dalle fonti degli eventi all'archivio registro eventi del server CA Enterprise Log Manager. Gli agenti utilizzano connettori per raccogliere i registri eventi da diverse fonti di eventi. Il seguente diagramma mostra le interazioni tra agenti e il server CA Enterprise Log Manager:



Dopo avere installato un agente su una fonte di eventi, è possibile configurare uno o più connettori affinché raccolgano eventi da fonti di eventi come periferiche, applicazioni, sistemi operativi e database. Gli esempi nel diagramma includono connettori per CA Access Control e un database Oracle. Solitamente si installa un solo agente per ogni server host o fonte di evento, ma è possibile configurare più di un tipo di connettore su tale agente. È possibile utilizzare l'Explorer agente che fa parte del server CA Enterprise Log Manager per controllare gli agenti e configurare e controllare i connettori su un agente. L'Explorer agente permette anche di creare gruppi di agenti per una gestione e un controllo più semplici.

Si basa la configurazione di un connettore su un'integrazione o su un listener, che sono modelli che comprendono file per l'accesso ai dati, l'analisi dei messaggi e il mapping dei dati. CA Enterprise Log Manager fornisce una serie di integrazioni pronte all'uso per fonti di eventi popolari.

È possibile trovare ulteriori informazioni e procedure per l'installazione di agenti nella *Guida all'installazione degli agenti CA Enterprise Log Manager*.

Ulteriori informazioni:

Visualizzazione e controllo dello stato di agenti o connettori (a pagina 218)

Utilizzo dell'Explorer agente

Subito dopo l'installazione di un server CA Enterprise Log Manager, un agente predefinito è elencato nell'Explorer agente. L'agente viene installato quando si installa il server CA Enterprise Log Manager e lo si utilizza per la raccolta di eventi diretta syslog.

L'Explorer agente traccia ed elenca gli agenti quando essi vengono installati in una rete e fornisce una posizione centralizzata perla configurazione, il comando e il controllo di agenti e connettori. Gli agenti vengono registrati con il server CA Enterprise Log Manager specificato al loro primo avvio. Quando avviene la registrazione, il nome dell'agente compare nell'Explorer agente e si è pronti per configurare un connettore per iniziare la raccolta dei registri eventi. I connettori raccolgono i registri eventi e li inviano al server CA Enterprise Log Manager. Un agente può controllare molti connettori.

L'utilizzo dell'Explorer agente per installare, configurare e controllare i connettori e gli agenti implica i seguenti passaggi di base:

1. Scaricare i file binari dell'agente.
2. Creare uno o più gruppi di agenti (facoltativo).
3. Creare e configurare un connettore, inclusa la creazione o l'applicazione delle regole di soppressione e riepilogo.
4. Visualizzare lo stato degli agenti o dei connettori.

Fare riferimento alla *Guida all'amministrazione di CA Enterprise Log Manager* per ulteriori informazioni sulla creazione e l'utilizzo di gruppi di agenti e connettori e su come applicare regole di soppressione agli agenti.

Ulteriori informazioni:

Informazioni sugli agenti (a pagina 68)
Informazioni sui gruppi di agenti (a pagina 68)
Informazioni sui connettori (a pagina 70)
Informazioni sui sensori di registro (a pagina 71)
Effetti della regola di soppressione (a pagina 73)

Configurazione dell'agente predefinito

L'installazione CA Enterprise Log Manager crea un agente predefinito sul server CA Enterprise Log Manager dotato di due connettori pronti all'uso, un connettore syslog_Connector e un connettore Linux_local. Il connettore syslog è disponibile per la raccolta di eventi syslog inviati al server CA Enterprise Log Manager. Il connettore Linux_local connector è disponibile per la raccolta di eventi a livello di sistema operativo dal server fisico CA Enterprise Log Manager o da un file syslog.

Nell'ambiente di base a due server, è necessario configurare uno o più connettori syslog sul server di raccolta per ricevere gli eventi.

La procedura per utilizzare l'agente predefinito include i seguenti passaggi:

1. (Facoltativo) Revisione delle integrazioni e dei listener syslog.
2. Creazione di un connettore syslog.
3. Verifica che il server CA Enterprise Log Manager stia ricevendo gli eventi syslog.

Revisione delle integrazioni e dei listener syslog.

È possibile rivedere le integrazioni e i listener syslog predefiniti prima di creare un connettore. I listener essenzialmente sono un modello dei connettori syslog che utilizzano integrazioni syslog specifiche fornite come contenuto pronto all'uso con il server CA Enterprise Log Manager.

Per analizzare le integrazioni syslog

1. Accedere a CA Enterprise Log Manager e alla scheda Amministrazione.
2. Fare clic sulla sottoscheda Library (Libreria) ed espandere il nodo Integrazione Log.
3. Espandere sia il nodo Integrazioni che il nodo Sottoscrizione.
4. Selezionare un'integrazione il cui nome termina con ..._Syslog.

   I dettagli dell'integrazione vengono visualizzati nella finestra sul lato destro. È possibile esaminare i file di analisi dei messaggi e i file di mapping dei dati utilizzato dall'integrazione, nonché altri dettagli quale la versione e l'elenco delle regole di soppressione e riepilogo.

Per analizzare un listener syslog

1. Espandere sia il nodo Listener che il nodo Sottoscrizione.
2. Selezionare il listener Syslog.

   I dettagli del listener predefinito vengono visualizzati nella finestra sul lato destro. È possibile esaminare dettagli quali le versioni, l'elenco delle regole di soppressione e riepilogo, le porte di attesa predefinite, l'elenco di host attendibili e il fuso orario del listener.

Creazione di un connettore syslog per l'agente predefinito

È possibile creare un connettore syslog per la ricezione di eventi syslog utilizzando l'agente predefinito sul server CA Enterprise Log Manager.

Per creare un connettore syslog per l'agente predefinito

1. Accedere a CA Enterprise Log Manager e alla scheda Amministrazione.
2. Espandere l'Explorer agente e un gruppo agente.

   L'agente predefinito viene installato automaticamente nel Gruppo agenti predefinito. È possibile spostare questo agente in un altro gruppo, se lo si desidera.

3. Selezione del nome dell'agente.

   L'agente predefinito ha lo stesso nome fornito al server CA Enterprise Log Manager durante l'installazione.

4. Fare clic su Crea nuovo connettore per aprire la procedura guidata del connettore.
5. Fare clic sull'opzione Listener e immettere un nome per questo connettore.
6. Applicare le regole di soppressione e di riepilogo in base alle proprie esigenze nella seconda e nella terza pagina della procedura guidata.
7. Selezionare una o più integrazioni syslog di destinazione nell'elenco Disponibile da utilizzare con questo connettore e spostarle nell'elenco Selezionate.
8. Impostare i valori delle porte UDP e TCP, se non si stanno utilizzando quelle predefinite, e fornire un elenco di host sicuri se l'implementazione li utilizza.

   Nota: se un agente CA Enterprise Log Manager non viene eseguito come root, esso non potrà aprire una porta inferiore a 1024. Il connettore syslog predefinito utilizza quindi la porta UDP 40514. L'installazione applica una regola di firewall al server CA Enterprise Log Manager per reindirizzare il traffico dalla porta 514 alla porta 40514.

9. Selezionare un fuso orario.
10. Fare clic su Salva e Chiudi per terminare il connettore.

    Il connettore inizierà la raccolta di eventi syslog che corrispondono alle integrazioni selezionate sulle porte specificate.

Verificare che CA Enterprise Log Manager stia ricevendo gli eventi syslog

È possibile verificare che il connettore sull'agente predefinito stia raccogliendo gli eventi syslog con la seguente procedura.

Per verificare la ricezione di un evento syslog

1. Accedere a CA Enterprise Log Manager e alla scheda Query e rapporti.
2. Selezionare la scheda Query di sistema e aprire la query Dettagli di tutti gli eventi.

   Dovrebbe essere possibile visualizzare gli eventi elencati per l'agente predefinito, se il connettore è stato configurato correttamente e la fonte dell'evento sta inviando eventi attivamente.

Esempio: Abilitazione della raccolta diretta tramite ODBCLogSensor

È possibile abilitare la raccolta diretta degli eventi generati da database specifici e prodotti CA mediante ODBCLogSensor. Per eseguire questa operazione, creare un connettore sull'agente predefinito basato su un'integrazione che utilizza ODBCLogSensor. Numerose integrazioni utilizzano questo sensore, ad esempio: CA_Federation_Manager, CAIdentityManager, Oracle10g, Oracle9i, e MS_SQL_Server_2005.

Di seguito si riporta una lista parziale dei prodotti che generano eventi disponibili per la raccolta diretta da parte dell'agente predefinito su un server CA Enterprise Log Manager. Per ogni prodotto, viene utilizzato un unico connettore e ciascun connettore utilizza ODBCLogSensor.

- CA Federation Manager
- CA SiteMinder
- CA Identity Manager
- Oracle 9i e 10g
- Microsoft SQL Server 2005

Per l'elenco completo, consultare la Matrice di integrazione del prodotto sul sito del Supporto in linea.

Questo esempio mostra la modalità per l'attivazione della raccolta diretta degli eventi da un database di Microsoft SQL Server. La distribuzione del connettore sull'agente predefinito si basa sull'integrazione MS_SQL_Server_2005. In questo esempio, il database SQL Server risiede in un server ODBC. Il connettore distribuito sull'agente CA Enterprise Log Manager esegue la raccolta degli eventi dalla tabella MSSQL_TRACE. L'abilitazione della raccolta eventi da un database Microsoft SQL Server include l'indirizzamento degli eventi selezionati verso tale tabella di traccia. La *Guida al connettore per Microsoft SQL Server*di CA include istruzioni specifiche per questa operazione.

Informazioni sulla modalità di configurazione dell'origine eventi di Microsoft SQL Server

1. Selezionare la scheda Amministrazione e la sottoscheda Library (Libreria).
2. Espandere Integrazione Log, Integrazioni e quindi Sottoscrizione e selezionare MS_SQL_Server_2005.

   La finestra Visualizza dettagli integrazione mostra il nome del sensore. ODBCLogSensor. Le piattaforme supportate includono Windows e Linux.
3. Fare clic sul collegamento alla Guida in linea della finestra Visualizza dettagli integrazione.

   Viene visualizzata al Guida al connettore per Microsoft SQL Server
4. Per ulteriori informazioni, consultare le sezioni relative ai prerequisiti e alla configurazione di Microsoft SQL Server.

Per configurare l'origine evento e verificare la registrazione

1. Raccogliere le seguenti informazioni: indirizzo IP del server ODBC, nome del database, nome utente e password dell'amministratore per l'accesso al server e credenziali dell'utente con privilegi ridotti utilizzate per l'autenticazione di SQL Server (definito dall'utente per l'accesso in sola lettura alla tabella di traccia).
2. Accedere al server ODBC con il nome utente e la password di amministratore.
3. Verificare la connettività su TCP/IP come specificato nella *Guida al connettore per Microsoft SQL Server*.
4. Configurare il server SQL e verificare l'indirizzamento degli eventi alla tabella di traccia come specificato nella *Guida al connettore per Microsoft SQL Server*.

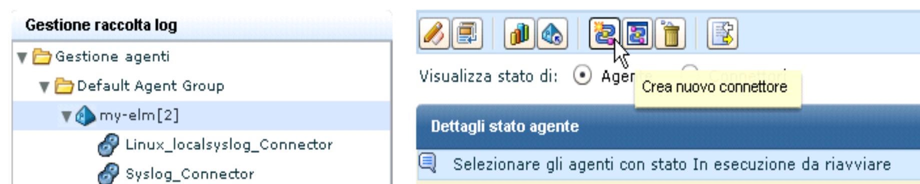
   Nota: registrare il nome del database in cui è stata creata la tabella di traccia. È necessario specificare il nome del database nella stringa di connessione. Ad esempio: master.

Per creare un connettore sull'agente predefinito e recuperare gli eventi generati da un database SQL Server su un server ODBC

1. Selezionare la scheda Amministrazione e la sottoscheda Raccolta log.
2. Espandere Gestione agenti, e il gruppo agenti contenente l'agente predefinito di CA Enterprise Log Manager
3. Selezionare un agente predefinito, ovvero un agente con il nome del server CA Enterprise Log Manager.

   È possibile eseguire la distribuzione di connettori diversi sull'agente predefinito.

4. Fare clic su Crea nuovo connettore.



   Viene aperta la creazione guidata nuovo connettore con il passaggio Dettagli connettore selezionato.

5. Selezionare l'integrazione MS_SQL_Server_2005 dall'elenco a discesa Integrazione.

   Il campo Nome connettore viene compilato con MS_SQL_Server_2005_Connector.

6. (Facoltativo) Sostituire il nome predefinito con un nome personalizzato per individuare più facilmente il connettore. Nel caso in cui il monitoraggio includa più database SQL Server con lo stesso agente, scegliere un nome univoco.

Creazione connettore
Immettere i dettagli richiesti
Tipo: Integrazioni Listener
Integrazione: MS_SQL_Server_2005
Nome connettore: MS_SQL_Server_2005_Connettore
Versione piattaforma: RHEL5 Controllo di versione piattaforma bypass

7. (Facoltativo) Fare clic su Applica regole di soppressione a, quindi selezionare le regole associate agli eventi supportati.

   Ad esempio, selezionare MSSQL_2005_Authorization 12.0.44.12.

8. Fare clic su Configurazione connettore e selezionare il collegamento della Guida in linea.

   Le Istruzioni includono i requisiti di configurazione del sensore per CA Enterprise Log Manager per Windows e Linux.

9. Consultare i passaggi per Linux, la piattaforma dell'agente predefinito e configurare la stringa di connessione e gli altri campi come specificato.

   a. Immettere la stringa di connessione specificata in Configurazione sensore--Linux, con il nome host o l'indirizzo IP dell' origine evento come indirizzo e il database SQL Server come database in MSSQLSERVER_TRACE

      `DSN=SQLServer Wire Protocol;Address=`*`IPaddress`*`,`*`port`*`;Database=`*`databasename`*

   b. Immettere il nome dell'utente con diritti di accesso in sola lettura per la raccolta eventi. Per disporre dell'accesso in sola lettura, l'utente deve essere assegnato a db_datareader e a ruoli pubblici.

   c. Immettere la password per il nome utente specificato.

   d. Specificare il fuso orario del database come offset GMT.

      Nota: sui server Windows, tali informazioni verranno visualizzate nella scheda Fuso orario delle proprietà di data e ora. Aprire l'orologio sulla barra delle applicazioni.

   e. Selezionare l'opzione Leggi dal principio se si desidera che il sensore log legga gli eventi dall'inizio del database. In caso contrario, deselezionare l'opzione.

   Di seguito si riporta un esempio parziale:

Configurazione sensore

Stringa di connessione:	DSN=SQLServer Wire Protocol;Address=172.24.36.107,1433;Database=master
Nome utente:	ELMsqlagent
Password:	********
Firma di differenza fuso orario:	-
Ore di differenza fuso orario:	5
Minuti di differenza fuso orario:	0
Nome log eventi:	MS_SQL_Server
Aggiorna percentuale di ancoraggio:	10
Intervallo di polling:	10
Numero massimo di eventi al secondo:	1000
	☑ Leggere dal principio

10. Fare clic su Salva, quindi su Chiudi.

    Il nuovo nome del connettore viene visualizzato sotto l'agente in Gestione agenti.



11. Fare clic su MS_SQL_Server_2005_Connector per visualizzare i dettagli dello stato.

    Inizialmente, lo stato visualizzato è Configurazione in sospeso. Attendere che lo stato sia In esecuzione.

Connettore	Agente	Gruppo agenti	Piattaforma	Integrazione	Stato
MS_SQL_Server_2005_Connettore	my-elm	Default Agent Group	Linux_X86_32	MS_SQL_Server_2005	In esecuzione

12. Selezionare il connettore e fare clic su In esecuzione per visualizzare i dettagli della raccolta eventi.

    Nota: è inoltre possibile eseguire un rapporto per visualizzare i dati del database.

Verificare che l'agente predefinito stia eseguendo la raccolta degli eventi dall'origine evento di destinazione

1. Selezionare la scheda Query e rapporti. Viene visualizzata la sottoscheda Query.
2. Espandere Prompt in Elenco query e selezionare Connettore.
3. Immettere il nome del connettore e fare clic su Vai a.

   Gli eventi raccolti vengono visualizzati. I primi due eventi visualizzati sono di tipo interno. Gli eventi successivi corrispondono agli eventi raccolti dalla tabella di traccia MS SQL configurata dall'utente.

   Nota: se gli eventi previsti non vengono visualizzati, fare clic su Filtri globali e Impostazioni dalla barra degli strumenti principale, impostare l'intervallo di tempo su Nessun limite, quindi salvare le impostazioni.

4. (Facoltativo) Selezionare Mostra eventi non elaborati ed esaminare la stringa risultato dei primi due eventi. La stringa risultato viene visualizzata alla fine dell'evento non elaborato. I valori riportati di seguito indicano l'avvio corretto.

   - result_string=ODBCSource initiated successfully - MSSQL_TRACE
   - result_string=<connector name> Connector Started Successfully

Esempio: Abilitazione della raccolta diretta tramite WinRMLinuxLogSensor

È possibile abilitare la raccolta diretta degli eventi generati da applicazioni Windows oppure dal sistema operativo Windows Server 2008 con WinRMLinuxLogSensor. Per eseguire questa operazione, creare un connettore sull'agente predefinito basato su un'integrazione che utilizza WinRMLinuxLogSensor. Numerose integrazioni utilizzano questo sensore, ad esempio: Active_Directory_Certificate_Services, Forefront_Security_for_Exchange_Server, Hyper-V, MS_OCS, e WinRM. L'applicazione e il sistema operativo Microsoft Windows che genera eventi recuperabili da WinRMLinuxLogSensor corrispondono ai sistemi per i quali è stata abilitata la Gestione remota Windows.

Di seguito si riporta una lista parziale dei prodotti che generano eventi disponibili per la raccolta diretta da parte dell'agente predefinito su un server CA Enterprise Log Manager. Per ogni prodotto, viene utilizzato un unico connettore e ciascun connettore utilizza WinRMLinuxLogSensor.

- Servizi certificati Microsoft Active Directory
- Microsoft Forefront Security per Exchange Server
- Microsoft Forefront Security per SharePoint Server
- Microsoft Hyper-V Server 2008
- Microsoft Office Communication Server
- Microsoft Windows Server 2008

Per l'elenco completo, consultare la Matrice di integrazione del prodotto sul sito del Supporto in linea.

Questo esempio mostra la modalità di abilitazione della raccolta diretta degli eventi mediante un connettore basato sull'integrazione WinRM. Quando tale connettore viene distribuito, esegue la raccolta degli eventi dall'origine evento di un sistema operativo Windows Server 2008 . La raccolta viene avviata dopo la configurazione delle origini evento per la registrazione degli eventi nel Visualizzatore eventi di Windows e l'abilitazione della Gestione remota Windows sul server, come specificato nella Guida del connettore associato all'integrazione.

Informazioni sulla modalità di configurazione dell'origine eventi di Windows Server 2008

1. Selezionare la scheda Amministrazione e la sottoscheda Library (Libreria).
2. Espandere Integrazione Log, Integrazioni e quindi Sottoscrizione e selezionare WinRM.

   La finestra Visualizza dettagli integrazione mostra il nome del sensore. WinRMLinuxLogSensor. Le piattaforme supportate includono Windows e Linux.
3. Fare clic sul collegamento alla Guida in linea della finestra Visualizza dettagli integrazione di WinRM.

   Viene visualizzata la Guida al connettore per Windows Server 2008--WinRM.

Per configurare l'origine evento e verificare la registrazione

1. Accedere all'host di destinazione con sistema operativo Windows Server 2008.

2. Attenersi alle istruzioni della *Guida al connettore per Microsoft SQL Server di CA* per verificare che gli eventi vengano visualizzati nel Visualizzatore eventi di Windows e per garantire che la Gestione remota Windows sia stata abilitata nel server di destinazione.

   Nota: questo processo richiede la creazione di un nome utente e di una password da immettere durante la configurazione del connettore. Tali credenziali concedono l'autenticazione richiesta per stabilire la connettività tra l'origine evento e CA Enterprise Log Manager.

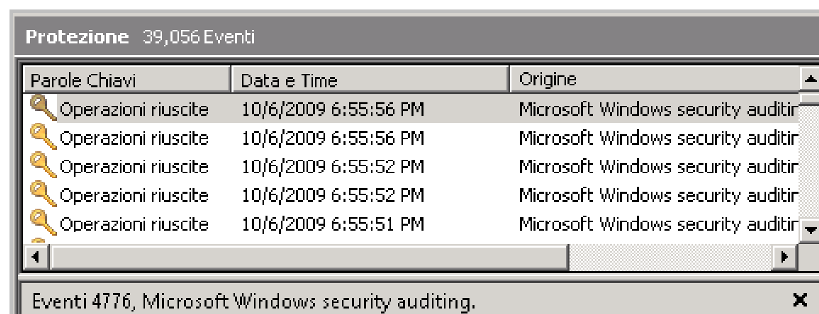
3. Verificare la registrazione.

   a. Aprire eventvwr dalla finestra di dialogo Esegui.

      Viene visualizzato il Visualizzatore eventi.

   b. Espandere Registri di Windows e fare clic su Protezione.

      Viene visualizzata la seguente schermata indicante che la registrazione è in corso.



Per abilitare la raccolta diretta degli eventi dalle origini evento di Windows

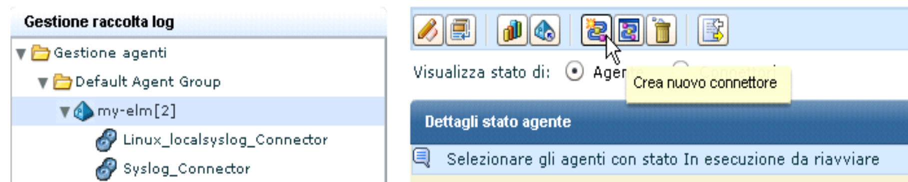
1. Selezionare la scheda Amministrazione e la sottoscheda Raccolta registri.

2. Espandere Gestione agenti da Gestione raccolta log ed espandere il gruppo agenti contenente l'agente predefinito di CA Enterprise Log Manager.

3. Selezionare un agente predefinito, ovvero un agente con il nome del server CA Enterprise Log Manager.

   È possibile eseguire la distribuzione di connettori diversi sull'agente predefinito.

4. Fare clic su Crea nuovo connettore.



Viene aperta la creazione guidata nuovo connettore con il passaggio Dettagli connettore selezionato.

5. Selezionare un'integrazione che utilizza il sensore log WinRM dall'elenco a discesa Integrazione.

   Ad esempio, selezionare WinRM.

   Creazione connettore
   Immettere i dettagli richiesti
   Tipo: Integrazioni Listener
   Integrazione: WinRM
   Nome connettore: WinRM_Connettore
   Versione piattaforma: RHEL5 Controllo di versione piattaforma bypass

   Il campo Nome connettore viene compilato con WinRM_Connector.

6. (Facoltativo) Fare clic su Applica regole di soppressione a, quindi selezionare le regole associate agli eventi supportati.

7. Fare clic su Configurazione connettore e selezionare il collegamento della Guida in linea.

   Le istruzioni includono la configurazione del sensore CA Enterprise Log Manager--WinRM.

   5.0 Configurazione del sensore CA Enterprise Log Manager, WinRM
   5.1 Parametro fisso

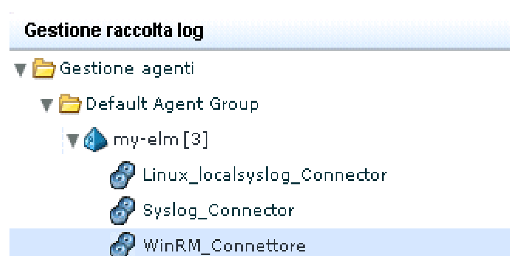
8. Per la configurazione del sensore, attenersi alle procedure riportate nella guida al connettore. Immettere l'indirizzo IP piuttosto che il nome host dell'host configurato per la Gestione remota Windows. Il nome utente e la password corrispondono alle credenziali aggiunte durante la configurazione della Gestione remota Windows.

   Di seguito viene riportato un esempio:

   Configurazione connettore
   Immettere i dettagli di configurazione
   Configurazioni salvate: Selezionare configuraz
   Configurazione sensore
   Nome computer: 172.24.36.107
   Porta: 80
   Nome utente: ELMagent
   Password: ********
   Nome log eventi: NT-Security
   Intervallo di polling: 10
   Aggiorna percentuale di ancoraggio: 10
   Leggere dal principio
   Nome origine: Security
   Nome canale (log): Security

9. Fare clic su Salva, quindi su Chiudi.

10. Il nuovo nome del connettore viene visualizzato sotto l'agente in Gestione agenti.



11. Fare clic su WinRM_Connector per visualizzare i dettagli di stato.

    Inizialmente, lo stato visualizzato è Configurazione in sospeso. Attendere che lo stato sia In esecuzione.

    Dettagli di stato

    Riavvia Avvia Interrompi

Connettore	Agente	Gruppo agenti	Piattaforma	Integrazione	Stato
WinRM_Connettore	my-elm	Default Agent Group	Linux_X86_32	WinRM	In esecuzione

12. Fare clic su Esegui per ottenere dati di aggregazione come EPS (eventi per secondo).

    Stato:
    CPU in percentuale: 0.0
    Utilizzo memoria in MB: 66.8
    EPS medio: 0
    Conteggio eventi filtrati: 0

Verificare che l'agente predefinito stia eseguendo la raccolta degli eventi dall'origine evento di destinazione

1. Selezionare la scheda Query e rapporti. Viene visualizzata la sottoscheda Query.
2. Espandere Prompt in Elenco query e selezionare Connettore.
3. Immettere il nome del connettore e fare clic su Vai a.
4. Visualizzare gli eventi raccolti.

Visualizzazione e controllo dello stato di agenti o connettori

È possibile monitorare lo stato degli agenti o dei connettori nell'ambiente, riavviare agenti e avviare, terminare e riavviare i connettori secondo le esigenze.

È possibile visualizzare agenti o connettori da livelli diversi della gerarchia della cartella Explorer agente. Ogni livello restringerà di conseguenza la visualizzazione disponibile:

- Dalla cartella Explorer agente è possibile visualizzare tutti gli agenti o i connettori assegnati al server CA Enterprise Log Manager corrente.
- Dalla cartella di uno specifico gruppo di agenti è possibile visualizzare gli eventi ed i connettori assegnati a tale gruppo agenti.
- Da un singolo agente è possibile visualizzare solo l'agente in questione ed i connettori ad esso assegnati.

La modalità FIPS (FIPS o non FIPS) per un agente può essere impostata da tutti e tre i livelli.

Per visualizzare lo stato degli agenti o dei connettori

1. Fare clic sulla scheda Amministrazione, e quindi sulla sottoscheda Raccolta registri.

   Verrà visualizzato l'elenco cartella di Raccolta registri.

2. Selezionare la cartella Explorer agente.

   Nel riquadro dei dettagli vengono visualizzati i pulsanti di gestione agente.

3. Fare clic su Stato e comando:

   Viene visualizzato il riquadro dello stato.

4. Selezionare Agenti o connettori.

   Comparirà il riquadro della ricerca degli agenti o connettori.

5. (Facoltativo) Selezionare i criteri di ricerca degli aggiornamenti degli agenti o dei connettori. Se non vengono immessi termini di ricerca, compariranno tutti gli aggiornamenti disponibili. Per restringere la propria ricerca, è possibile selezionare uno o più criteri fra i seguenti:
   - Gruppo agenti: restituisce solo gli agenti ed i connettori assegnati al gruppo selezionato.
   - Piattaforma: restituisce solo gli agenti ed i connettori in esecuzione sul sistema operativo selezionato.
   - Modello nome agente: restituisce solo gli agenti e i connettori contenenti il modello specificato.
   - (Solo connettori) Integrazione: restituisce solo i connettori utilizzando l'integrazione selezionata.
6. Fare clic su Mostra stato.

   Verrà visualizzato un grafico dei dettagli, che visualizza lo stato degli agenti o dei connettori corrispondenti alla ricerca dell'utente. Ad esempio:

   ```
   Totale: 10 In esecuzione: 8 In sospeso: 1 Terminati: 1 Non risponde: 0
   ```
7. (Facoltativo) Fare clic sulla visualizzazione dello stato per visualizzare i dettagli nel riquadro Stato in fondo al grafico

   Nota: è possibile fare clic sul pulsante Su richiesta di un agente o un connettore per aggiornare la visualizzazione dello stato.
8. (Facoltativo) Se si stanno visualizzando i connettori, selezionare qualsiasi connettore e fare clic su Ravvia, Avvia o Interrompi. Se si stanno visualizzando gli agenti, selezionare qualsiasi agente e fare clic su Riavvia.

Capitolo 7: Creazione di federazioni

Questa sezione contiene i seguenti argomenti:

Query e rapporti in un ambiente federato

Un unico server CA Enterprise Log Manager restituisce i dati dal database di eventi interni per rispondere alle query e popolare i rapporti. Se si dispone di una federazione di server CA Enterprise Log Manager, è possibile controllare come query e rapporti restituiscono le informazioni sugli eventi dal modo in cui si configurano le relazioni della federazione. È inoltre possibile conservare i risultati delle query dai singoli server disabilitando l'impostazione globale Usa query federate.

Per impostazione predefinita, l'impostazione globale Usa query federate è abilitata. In questo modo le query da un server CA Enterprise Log Manager genitore vengono inviate a tutti i server CA Enterprise Log Manager figlio. Ogni server CA Enterprise Log Manager figlio interroga l'archivio registro eventi attivo e il catalogo dell'archivio oltre a tutti i server CA Enterprise Log Manager figlio. Ogni server CA Enterprise Log Manager figlio crea un unico set di risultati da inviare al server CA Enterprise Log Manager genitore che invia la richiesta. La protezione da query circolari è incorporata in CA Enterprise Log Manager per abilitare le configurazioni a coppie.

L'implementazione di CA Enterprise Log Manager tipica per un'azienda ha da uno a cinque server. L'implementazione di una grande azienda può avere dieci o più server. Il modo in cui si configura la federazione controlla quante informazioni sono visibili nel server CA Enterprise Log Manager che produce la query. Il tipo più semplice di query deriva dal server CA Enterprise Log Manager principale e restituisce le informazioni di tutti i server figlio configurati al di sotto di esso.

Quando si interroga la federazione da un server figlio, i risultati visualizzati dipendono dalla configurazione della federazione. In una federazione *gerarchica*, tutti i server configurati come figlio sotto al di sotto di un server restituiscono ad esso i risultati della query. In una federazione a *coppie*, tutti i server interconnessi restituiscono i dati al server che produce la query.

Federazioni gerarchiche

Le *federazioni gerarchiche* utilizzano una struttura a piramide rovesciata per distribuire i carichi della raccolta di eventi su un'ampia area. La struttura è simile al grafico di un'organizzazione. Non esiste un numero di livelli impostato da creare: è possibile creare i livelli che hanno più senso per le esigenze della propria azienda.

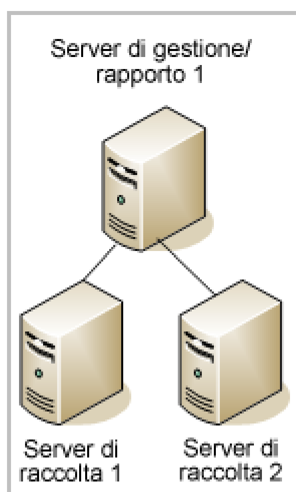
In una federazione gerarchica, è possibile connettersi a ogni server CA Enterprise Log Manager per visualizzare i rapporti sui dati degli eventi e i dati dei server figlio al di sotto. L'estensione dei dati a cui si può accedere è limitata da dove si inizia la gerarchia. Se si inizia al centro della gerarchia, è possibile visualizzare solo i dati del server e i dati di ogni server figlio. Più ci si sposta in alto nella gerarchia di una federazione, più sarà ampia l'estensione dei dati della rete disponibili. Al livello massimo, si ha accesso a tutti i dati dell'intera distribuzione.

Le federazioni gerarchiche sono utili, ad esempio, in distribuzioni regionali. Supponiamo di volere che le risorse locali abbiano accesso ai dati degli eventi all'interno di una certa gerarchia, o ramo, della rete, ma non ai dati degli eventi in altri rami paralleli. Si può creare una federazione gerarchica con due o più rami paralleli per contenere i dati per ogni regione. Ognuno dei rami può inviare rapporti a un server di gestione CA Enterprise Log Manager presso l'ufficio della sede centrale per una visualizzazione dall'alto al basso di tutti i rapporti del registro eventi.

Esempio di federazione gerarchica

Nella mappa della federazione mostrata nel diagramma che segue, la rete utilizza il server CA Enterprise Log Manager di gestione come server di rapporto e diversi server di raccolta in una configurazione simile ad un grafico organizzativo. Il server di gestione/dei rapporti agisce come server CA Enterprise Log Manager genitore e fornisce autenticazione utenti, autorizzazioni e funzioni di gestione principali oltre a funzioni di rapporto della gestione delle query, rapporti e avvisi. I server di raccolta in questo esempio sono i figli del server di gestione/dei rapporti 1. È possibile predisporre livelli aggiuntivi nella gerarchia. Tuttavia, non può essere presente più di un server di gestione. I livelli aggiuntivi saranno composti da server di rapporto genitori dei server di raccolta.

Come esempio di questo tipo di federazione, il server di gestione/raccolta 1 può essere posizionato negli uffici della sede, con server di raccolta posizionati in uffici regionali o delle filiali rappresentati dal server di raccolta 1 e 2. Ogni ramo può ricevere le informazioni dei rapporti sui propri dati, ma non i dati dell'altro ramo. Ad esempio, dal server di raccolta 1, è possibile avere query e rapporti solo sui dati nel server di raccolta 1. Dal server di gestione/raccolta 1, tuttavia, è possibile avere query e rapporti sui dati nel server di gestione/raccolta 1, nel server di raccolta 1 e nel server di raccolta 2.



In una federazione gerarchica, ogni server CA Enterprise Log Manager può avere uno o più figli, ma solo un genitore. Si configura questo tipo di federazione in un modo dall'alto al basso, iniziando con il server di gestione. Quindi si passa attraverso ogni layer dall'alto al basso per configurare i server di rapporto e di raccolta figlio. La parte essenziale per la configurazione di una federazione consiste nella creazione di una mappa dei server e delle relazioni pianificate. Quindi è possibile configurare un server CA Enterprise Log Manager come server figlio, per implementare le relazioni tra di essi.

Federazioni a coppie

Una *federazione a coppie* è simile a una federazione gerarchica poiché può avere dei livelli. La differenza fondamentale è nella configurazione delle connessioni tra i server. Una federazione a coppie può permettere a qualsiasi server CA Enterprise Log Manager nella rete di eseguire query e rapporti dei dati di tutti gli altri server CA Enterprise Log Manager. Le possibilità di rapporto dipendono dalle relazioni create tra i server.

Ad esempio, in una federazione a coppie, i server potrebbero interconnettersi solo in un ramo verticale. Ciò significa che tutti i server CA Enterprise Log Manager in tale ramo avranno accesso a tutti gli altri server CA Enterprise Log Manager nello stesso ramo. Ciò è in contrasto diretto con un server CA Enterprise Log Manager in una federazione gerarchica, che può produrre rapporti solo sui server al di sotto di esso nella gerarchia.

In una formazione ad anello o a stella, ogni server CA Enterprise Log Manager è configurato per essere figlio di tutti gli altri server. Quando si richiede il rapporto dei dati da qualsiasi server CA Enterprise Log Manager, si visualizzano i dati di tutti i server CA Enterprise Log Manager all'interno della rete.

La federazione a coppie assegna due o più server CA Enterprise Log Manager come primari e utilizza i server in una federazione a prescindere dalla loro posizione all'interno della rete. Anche i server configurati *come* figlio sono configurati per visualizzare i figli nello stesso ramo o in altri rami come federati ad essi. Ad esempio, se si dispone di due server CA Enterprise Log Manager, A e B, è possibile creare una federazione a coppie rendendo B figlio di A, *e* A figlio di B. Questa è la configurazione prevista quando si utilizzano due o più server di gestione.

Esempio di federazione a coppie

Esaminare la seguente illustrazione di una federazione a coppie completa:

Nella federazione a coppie mostrata in questo diagramma, quattro server di raccolta sono in federazione l'uno con l'altro e con entrambi i server di rapporto. Ogni server è sia genitore che figlio di ogni altro server nella federazione.

Un vantaggio potenziale di questa distribuzione rispetto alla federazione strettamente gerarchica è la possibilità di accedere ai dati da qualsiasi punto all'interno della coppia e di ottenere i risultati da tutti gli altri server CA Enterprise Log Manager nella coppia, a prescindere dalla gerarchia.

È possibile unire federazioni a copie e gerarchiche per definire la configurazione che si adatta meglio alle proprie esigenze. Ad esempio, una configurazione a coppie all'interno di un singolo ramo potrebbe risultare molto utile per distribuzioni globali. È possibile ottenere una panoramica globale dei dati dai server di rapporto genitore, mantenendo cluster regionali (rami) che hanno accesso solo ai propri dati.

Configurazione di una federazione CA Enterprise Log Manager

Ogni server CA Enterprise Log Manager che viene aggiunto alla federazione deve fare riferimento allo stesso nome dell'istanza dell'applicazione sul server di gestione. In questo modo, il server di gestione può archiviare e gestire assieme tutte le configurazioni come configurazioni globali.

È possibile configurare la federazione in qualsiasi momento, ma è utile eseguire questa operazione prima di iniziare la pianificazione dei rapporti, se si desiderano rapporti consolidati.

La configurazione di una federazione include le seguenti operazioni:

1. Creare una mappa della federazione.
2. Installare il primo CA Enterprise Log Manager, il server di gestione.
3. Installare uno o più server aggiuntivi.
4. Configurare le relazioni genitore/figlio. Ad esempio, iniziare selezionando i figli della federazione del server di gestione dalle impostazioni di archiviazione dei registri eventi di questo server.

   Il primo gruppo di server figlio forma il secondo strato, o livello, della federazione se si sta configurando una federazione gerarchica.
5. Visualizzare il grafico della federazione per verificare che la struttura tra i server nei livelli genitore e figlio sia configurata correttamente.

Configurazione di un server CA Enterprise Log Manager come server figlio

La configurazione di un server CA Enterprise Log Manager come figlio di un altro server è il passaggio fondamentale nella creazione di una federazione. Utilizzare questa procedura per aggiungere server alla federazione in qualsiasi momento. È necessario installare tutti i server CA Enterprise Log Manager che si desidera federare utilizzando lo stesso nome dell'istanza dell'applicazione registrato prima di eseguire questa parte della configurazione. Quando si installa un nuovo server, il suo nome appare nell'elenco dei server disponibili della federazione. È possibile eseguire questa procedura tutte le volte che è necessario per creare la struttura federata desiderata.

Per configurare un server CA Enterprise Log Manager come server figlio

1. Eseguire l'accesso a uno dei server CA Enterprise Log Manager registrato con lo stesso nome dell'istanza dell'applicazione degli altri nella federazione desiderata.
2. Fare clic sulla scheda Amministrazione e selezionare la sottoscheda Servizi.
3. Espandere la cartella del servizio archivio registro eventi e selezionare il nome del server CA Enterprise Log Manager genitore.
4. Scorrere verso il basso fino all'elenco Figlio della federazione.
5. Selezionare uno o più nomi di server da configurare come figli del server genitore dai server presenti nell'elenco Disponibile.
6. Utilizzare i pulsanti a forma di freccia per spostare le selezioni nell'elenco dei server selezionati.

   I server CA Enterprise Log Manager selezionati e spostati nell'elenco sono ora figli federati del server genitore.

Ulteriori informazioni:

Selezione dell'utilizzo di query federate (a pagina 155)

Visualizzazione del grafico di una federazione e monitoraggio dello stato del server

È possibile visualizzare un grafico che mostra i server CA Enterprise Log Manager nell'ambiente, le relazioni di federazione e le informazioni sullo stato dei server individuali. Il grafico della federazione permette di visualizzare la struttura corrente della federazione e i dettagli di ogni server. È possibile inoltre selezionare il server locale a cui vengono inviate le query nella sessione, configurandolo come server padre.

Per visualizzare il grafico della federazione, fare clic su Mostra grafico federazione e Monitoraggio stato nella parte superiore della schermata:

Verrà visualizzata una finestra che mostra una rappresentazione grafica di tutti gli host dell'archivio eventi registrati con il server di gestione corrente:

- Gli archivi eventi con i figli della federazione sono visualizzati in azzurro, collegati da righe nere che mostrano la relazione della federazione.
- Gli archivi di eventi senza figli della federazione sono visualizzati in verde chiaro.

È possibile selezionare un server locale corrente per le finalità di query.

È inoltre possibile visualizzare i dettagli dello stato per i server visualizzati. Fare clic su un server nel grafico della federazione per visualizzare le schermate con i dettagli dello stato, compresi:

- Percentuale di utilizzo della CPU
- Percentuale di utilizzo della memoria disponibile
- Percentuale di utilizzo dello spazio su disco disponibile
- Eventi ricevuti al secondo
- Grafico principale sullo stato dell'archivio di registro eventi

Ulteriori informazioni:

Esempio: mappa della federazione per un'impresa di medie dimensioni (a pagina 40)
Esempio: mappa federazione di una grande impresa (a pagina 38)

Capitolo 8: Lavorare con la libreria di perfezionamento eventi

Questa sezione contiene i seguenti argomenti:

Informazioni sulla libreria di perfezionamento eventi

La libreria di perfezionamento eventi fornisce strumenti per creare nuovi file di analisi e di mapping o per modificare le copie di quelli esistenti per fornire supporto per nove periferiche, applicazioni e altro ancora. La libreria include le seguenti opzioni:

- Integrazioni
- Listener
- File di mapping e analisi
- Regole di soppressione e di riepilogo

Le regole di soppressione impediscono la raccolta dei dati o impediscono di inserirli nell'archivio registro eventi. Le regole di riepilogo permettono di aggregare gli eventi per ridurre il numero di inserimenti per tipi di eventi o azioni simili. Questa è la parte più utilizzata della libreria poiché le regole di soppressione e di riepilogo possono aiutare a ottimizzare le prestazioni della rete e del database.

È possibile utilizzare l'area delle integrazioni per visualizzare integrazioni predefinite e per creare nuove integrazioni per periferiche, applicazioni, file o database personalizzati o proprietari. Ulteriori informazioni sono disponibili nella *Guida all'amministrazione di CA Enterprise Log Manager* e nella guida online.

Supporto di nuove fonti eventi con la libreria di perfezionamento eventi

Per supportare un dispositivo, un'applicazione, un database o un'altra origine eventi che non sia già supportata, è possibile utilizzare le procedure guidate di mapping e analisi dei file e le procedure guidate di integrazione per creare i componenti necessari.

Il processo comprende i seguenti passaggi generali:

1. Creazione di file di analisi per raccogliere i dati degli eventi come coppie nome-valore
2. Creazione di file di mapping per mappare le coppie nome-valore nella grammatica evento comune
3. Creazione di nuove integrazioni e listener per raccogliere i dati dalla fonte di eventi.

I file di integrazione, analisi e mapping e le regole di riepilogo sono descritte dettagliatamente nella *Guida all'amministrazione CA Enterprise Log Manager* e nella guida online.

File di mapping e analisi

Durante il funzionamento, CA Enterprise Log Manager legge gli eventi in ingresso e li suddivide in sezioni in un'azione chiamata *analisi*. Esistono file di analisi dei messaggi separati per diverse periferiche, sistemi operativi, applicazioni e database. Quando gli eventi in ingresso vengono analizzati in coppie nome-valore, tali dati passano attraverso un modulo di *mapping* che posiziona i dati degli eventi nei campi all'interno del database.

Il modulo di mapping utilizza i file di mapping dei dati creati per fonti specifiche degli eventi simili ai file di analisi dei messaggi. Lo schema del database è la grammatica evento comune che rappresenta una delle funzioni centrali di CA Enterprise Log Manager.

L'analisi e il mapping assieme sono i mezzi attraversi cui i dati vengono normalizzati e archiviati in un database comune a prescindere dal tipo di evento o dal formato del messaggio.

L'integrazione guidata e alcuni moduli di Adapter CA richiedono la configurazione dei file di mapping e analisi che descrivono al meglio il tipo di dati degli eventi per cui un connettore o un adapter è in ascolto. Nei riquadri della configurazione dove compaiono questi controlli, l'ordine dei file di analisi dei messaggi deve riflettere il numero relativo di eventi ricevuto di questo tipo. L'ordine dei dati dei file di mapping dei dati deve riflettere anche la quantità di eventi ricevuti da una determinata fonte.

Ad esempio, se un modulo listener di syslog di un server CA Enterprise Log Manager specifico riceve principalmente eventi Cisco PIX Firewall, è necessario inserire prima i file CiscoPIXFW.XMPS e CiscoPIXFW.DMS nel rispettivo elenco.

Appendice A: Considerazioni per gli utenti CA Audit

Questa sezione contiene i seguenti argomenti:

Comprendere le differenze delle architetture

Nella pianificazione di come utilizzare CA Audit e CA Enterprise Log Manager assieme, prima è necessario comprendere le differenze delle architetture e gli effetti che esse hanno sulla struttura della rete.

CA Enterprise Log Manager utilizza un registro eventi incorporato e fornisce un Explorer agente per configurare e gestire gli agenti. La nuova tecnologia abbinata a una grammatica evento comune consente un trasferimento più veloce degli eventi nell'archivio supportando un numero maggiore di fonti di eventi. La grammatica evento comune permette CA Enterprise Log Manager di normalizzare gli eventi da fonti di eventi diverse in un singolo schema di database.

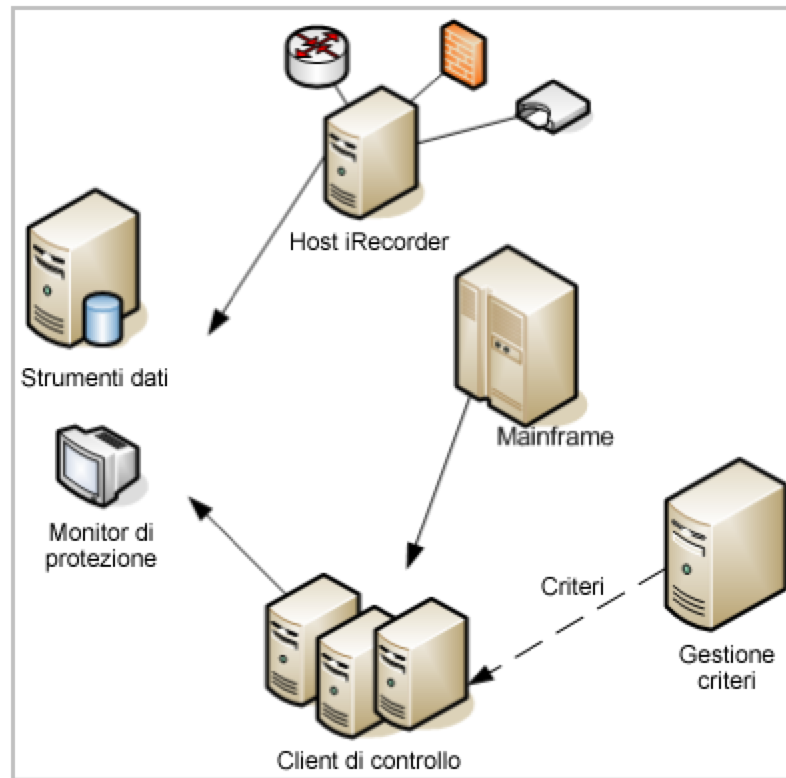
CA Enterprise Log Manager si integra a un certo livello CA Audit, ma per progettazione non è completamente interoperabile. CA Enterprise Log Manager è un'infrastruttura server nuova e separata in grado di essere in funzione parallelamente a CA Audit, con le seguenti considerazioni sulla gestione degli eventi:

CA Enterprise Log Manager può...	CA Enterprise Log Manager *non* può...
Ricevere registri di eventi inviati dai client CA Audit e da iRecorder utilizzando listener configurabili.	Accedere direttamente a registri di eventi archiviati nel database del collector CA Audit.
Fornire un'utilità per importare i dati del registro eventi archiviati nel database del collector CA Audit (tabella SEOSDATA).	

CA Enterprise Log Manager può...	CA Enterprise Log Manager *non* può...
Utilizzare agenti per inviare registri eventi solo all'infrastruttura del server CA Enterprise Log Manager.	
Permettere agli agenti CA Enterprise Log Manager e ai client CA Audit con iRecorder di essere in funzione sullo stesso host fisico.	Permettere agli agenti CA Enterprise Log Manager e ai client CA Audit con iRecorder sullo stesso host di accedere simultaneamente alle stesse fonti di registri.
Utilizzare l'Explorer agente incorporato per gestire solo agenti CA Enterprise Log Manager. Durante il funzionamento fianco a fianco dei due sistemi, CA Audit utilizza il proprio Gestore dei criteri solo per gestire client CA Audit	
	Trasferire dati CA Audit contenuti in raccoglitori a tabella, modello di rapporti o rapporti personalizzati, criteri di avviso, criteri di raccolta/filtraggio o criteri di controllo degli accessi basati sui ruoli

Architettura di CA Audit

La seguente illustrazione mostra un'implementazione semplificata di CA Audit:



In alcune distribuzioni aziendali di CA Audit, i dati degli eventi sono archiviati dal servizio di raccolta in un database relazionale in esecuzione nel server Data Tools. Un amministratore del database controlla ed esegue la manutenzione di questo database e lavora con un amministratore di sistema per garantire che i criteri corretti siano applicati per raccogliere gli eventi desiderati e per escludere eventi non necessari.

Le righe continue in questo diagramma mostrano gli eventi che passano da client e recorder CA Audit e host di iRecorder al server Data Tools o in alcuni casi ad una console di monitoraggio di sicurezza opzionale. Una linea tratteggiata rappresenta il flusso di controllo tra il server del Gestore dei criteri e i client che utilizzano i criteri.

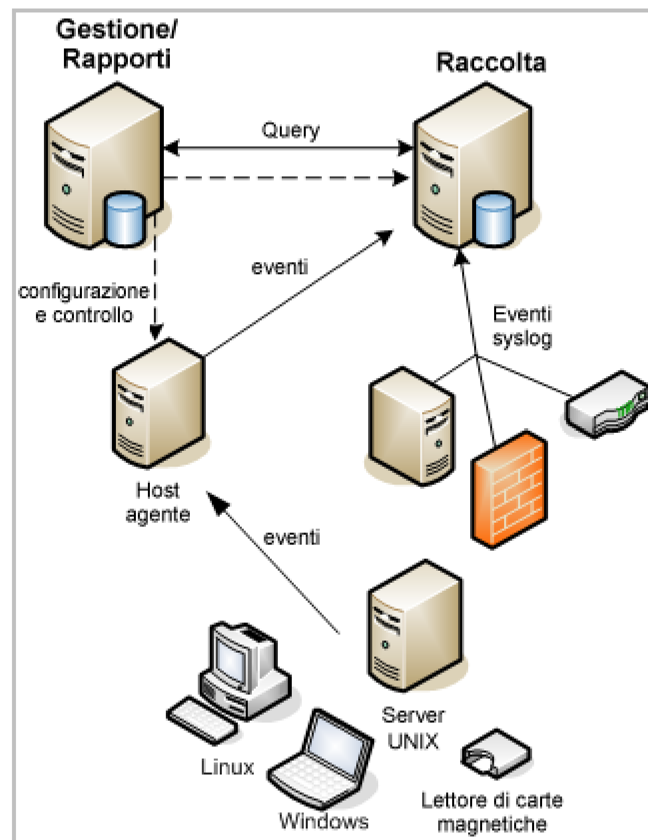
Il server Data Tools fornisce utilità di base di rapporti e di visualizzazione oltre all'archiviazione eventi. Query e rapporti personalizzati sono la norma in implementazioni aziendali e richiedono molto tempo per la creazione e la manutenzione.

Questa topologia della rete permette la raccolta di una serie di tipi di eventi da diverse periferiche, applicazioni e database. Si dispone dell'archivio centrale degli eventi raccolti che di solito fa parte o è gestito dal server Data Tools, che offre anche alcuni rapporti.

Tuttavia, sono necessarie funzioni aggiuntive per scalare la soluzione per gestire rapidamente volumi di eventi in aumento. È necessario generare rapporti che dimostrino la conformità con una serie di normative federali e internazionali. È necessario essere in grado di trovare i rapporti rapidamente e velocemente.

Architettura di CA Enterprise Log Manager

La seguente illustrazione mostra un'implementazione di base a due server di CA Enterprise Log Manager:



Un sistema CA Enterprise Log Manager può avere uno o più server, laddove il primo server installato è il server di gestione. Non può essere presente più di un server di gestione in un sistema, ma è possibile avere diversi sistemi. Il server di gestione conserva contenuti e configurazione di tutti i server CA Enterprise Log Manager ed esegue l'autorizzazione e l'autenticazione degli utenti.

In un'implementazione di base costituita da due server, il server di gestione assume anche il ruolo di server di rapporto. Un server di rapporto riceve eventi trattati da uno o più server di raccolta. Il server di rapporto gestisce query e rapporti su richiesta oltre ad avvisi e rapporti pianificati. Il server di raccolta tratta gli eventi raccolti.

Ogni server CA Enterprise Log Manager dispone del proprio database dell'archivio registro eventi interno. L'archivio del registro eventi è n database proprietario che utilizza la compressione per migliorare la capacità di archiviazione e per consentire le query di file dei database attivi, di file contrassegnati per l'archiviazione e file defrosted. Non è necessario nessun pacchetto DBMS relazionale per l'archiviazione di eventi.

Il server CA Enterprise Log Manager di raccolta può ricevere eventi direttamente utilizzando il proprio agente predefinito o da un agente che risiede sulla fonte dell'evento. Gli agenti possono risiedere anche su un host che agisce come raccoglitore per altre fonti di eventi nella rete, come un concentratore VPN o un host router.

Le righe continue in questo diagramma rappresentano i flussi di eventi dalle fonti di eventi agli agenti al server di raccolta al ruolo dei rapporti del server di gestione o dei rapporti. Le linee tratteggiate mostrano il traffico di configurazione e di controllo tra i server CA Enterprise Log Manager e dal ruolo di gestione del server di gestione o dei rapporti agli agenti. È possibile utilizzare qualsiasi server CA Enterprise Log Manager nella rete per controllare ogni agente nella rete, fintanto che i server CA Enterprise Log Manager erano registrati con lo stesso nome di istanza dell'applicazione nel server di gestione durante l'installazione.

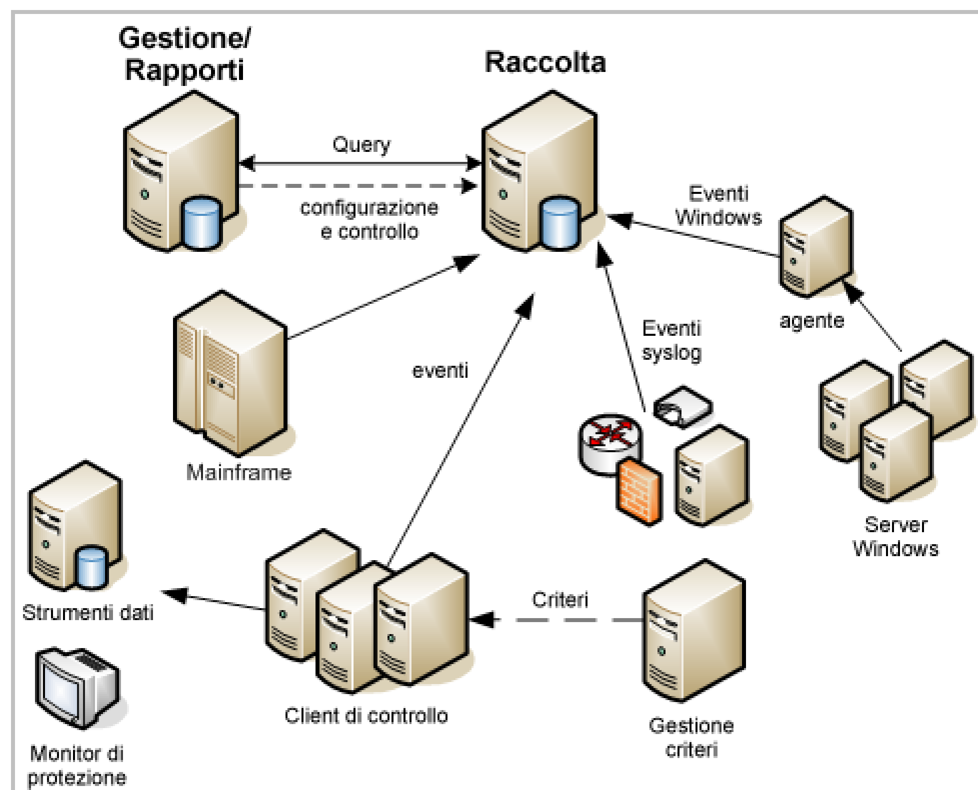
Gli agenti utilizzano connettori (non mostrati) per raccogliere gli eventi. Un unico agente può gestire diversi connettori per raccogliere molti tipi diversi di eventi contemporaneamente. Ciò significa che un unico agente distribuito su una fonte di eventi singola può raccogliere tipi diversi di informazioni. Il server CA Enterprise Log Manager offre anche listener che permettono la raccolta di eventi da altre applicazioni CA utilizzando iRecorder e recorder SAPI esistenti dalla rete CA Audit.

È possibile federare i server CA Enterprise Log Manager per scalare la soluzione e condividere i dati dei rapporti tra di essi senza dovere trasportare i dati all'esterno dei confini. Ciò può fornire una visualizzazione della conformità a livello di rete seguendo sempre le normative sul mantenimento delle posizioni dei dati fisici.

Aggiornamenti delle sottoscrizioni per query e rapporti predefiniti rappresentano la possibilità di non dover più effettuare manualmente la manutenzione di query e rapporti. Le procedure guidate fornite permettono di creare le proprie integrazioni personalizzate per periferiche e applicazioni di terze parti non ancora supportate.

Architettura integrata

Il seguente diagramma mostra una rete CA Audit tipica con CA Enterprise Log Manager aggiunto per utilizzare al meglio le capacità di gestione di grandi volumi di eventi e di rapporti basati sulla conformità:



CA Enterprise Log Manager utilizza un Explorer agente integrato, un archivio registro eventi incorporato e un'unica interfaccia utente per centralizzare e semplificare la raccolta dei registri. La tecnologia dell'agente CA Enterprise Log Manager abbinata a una grammatica evento comune consente un trasferimento più veloce degli eventi nell'archivio gestendo un numero maggiore di fonti di eventi. Un unico agente può gestire diversi connettori alle fonti degli eventi, semplificando le attività di gestione degli agenti e sfruttando integrazioni predefinite per fonti di registri eventi note o comuni.

In questa implementazione, il server di raccolta CA Enterprise Log Manager riceve direttamente gli eventi syslog, basati su iTechnology e del recorder SAPI. Il server di raccolta riceve gli eventi da fonti di eventi Windows attraverso un agente CA Enterprise Log Manager separato basato su Windows. È possibile avere diversi agenti distribuiti nella rete, ognuno dei quali è in grado di raccogliere molti tipi diversi di dati di eventi attraverso i connettori. Ciò può aiutare a ridurre il traffico di eventi al database SEOSDATA e a utilizzare al meglio query e rapporti disponibili in CA Enterprise Log Manager. Una semplice modifica di regole dei criteri permette ai client CA Audit di inviare gli eventi raccolti sia al server Data Tools che al server CA Enterprise Log Manager.

Oltre a una velocità superiore, CA Enterprise Log Manager offre query e rapporti pronti all'uso che aiutano a dimostrare la conformità rispetto a standard diversi come PCI (DSS) e SOX. Quando si abbinano le query e i rapporti predefiniti all'implementazione CA Audit e CA Security Command Center esistente, è possibile utilizzare al meglio gli investimenti nelle soluzioni personalizzate sfruttando i rapporti e l'elevata velocità di CA Enterprise Log Manager.

Configurazione degli adattatori CA

Gli adattatori CA sono un gruppo di listener che riceve eventi da componenti di CA Audit come i client CA Audit, i recorder iRecorder e SAPI nonché le origini evento che inviano gli eventi con iTechnology.

Impostare le opzioni di configurazione dell'adapter CA prima di modificare le configurazioni dei criteri di CA Audit o iRecorder. Ciò assicura che i processi dei listener siano operativi prima dell'arrivo degli eventi. Ciò impedisce la mappatura errata dei dati degli eventi.

Se si inviano eventi attraverso iRecorder a CA Audit, o se si utilizza un client CA Audit con iRecorder, si utilizzeranno gli adapter SAPI CA Enterprise Log Manager per ricevere eventi. Per inviare eventi a CA Enterprise Log Manager, si dovranno modificare i criteri CA Audit per gli eventi CA Access Control. È possibile aggiungere un'azione Collector o Route ad una regola esistente.

- Se si crea un'azione Collector su una regola in un criterio CA Audit esistente, configurare l'adapter CA Collector SAPI per ricevere gli eventi.
- Se si crea un'azione Route su una regola in un criterio CA Audit esistente, configurare l'adapter CA Route SAPI per ricevere gli eventi.

Fare riferimento alla documentazione di origine SAPI per istruzioni sulla riconfigurazione per inviare eventi direttamente a CA Enterprise Log Manager.

Se si ha intenzione di installare un iRecorder autonomo o di utilizzare un iRecorder esistente, si dovrà configurare il plug-in eventi iTech per ricevere gli eventi. Ad esempio, utilizzare questo approccio se CA Audit non è installato, ma si vuole utilizzare un iRecorder CA per raccogliere eventi da una fonte di eventi supportata. La procedura include i seguenti passaggi:

- Configurazione del plug-in eventi iTechnology
- Configurare il prodotto in base ad iRecorder o iTechnology per inviare eventi direttamente al server CA Enterprise Log Manager

Informazioni su SAPI Router e Collector

I servizi SAPI sono usati solitamente per ricevere eventi dai client e dai prodotti CA Audit esistenti. CA Enterprise Log Manager utilizza due istanze del servizio listener SAPI, una installata come SAPI Collector, l'altra come SAPI Router.

I moduli SAPI utilizzano il daemon iGateway per il comando e il controllo. I moduli agiscono come router SAPI e un collector SAPI utilizza porte statiche o dinamiche attraverso portmapper.

Utilizzare il collector SAPI durante l'invio di eventi dai client CA Audit in modo che sia possibile utilizzare il supporto di fail-over incorporato nell'azione Audit Collector.

Utilizzare il router SAPI durante l'invio di eventi dai client CA Audit utilizzando l'azione Route o quando si inviano eventi dai recorder o dalle integrazioni SAPI che supportano l'invio di eventi direttamente a un client CA Audit. In questo caso si configura il mittente remoto come se il server CA Enterprise Log Manager fosse il client CA Audit.

Il listener SAPI apre la propria porta e ascolta passivamente affinché i nuovi eventi vengano inviati ad esso. Ogni istanza del modulo SAPI dispone della propria configurazione che specifica quanto segue:

- Porta sui cui ascoltare
- File di mapping dei dati (DM) da caricare
- Librerie di crittografia da utilizzare

Dopo avere ricevuto questo evento, il modulo lo invia alla libreria di mapping e CA Enterprise Log Manager lo inserisce all'interno del database.

Importante: la libreria di mapping dei dati può contenere uno o più file di mapping con lo stesso nome, ma numeri di versione diversi. I file diversi supportano diversi livelli di rilascio della stessa fonte eventi di eventi, come un sistema operativo, un database e così via. È essenziale selezionare solo un file di mapping specifico per la versione quando si configura il collector o il router SAPI.

Se due file con lo stesso nome sono presenti nell'elenco dei file di mapping selezionati, il motore di mapping utilizza solo il primo dell'elenco. Se non si tratta del file corretto per il flusso di eventi in ingresso, il motore di mapping non sarà in grado di mappare correttamente l'evento. Ciò a sua volta potrebbe provocare da parte delle query e dei rapporti la visualizzazione di informazioni che non includono gli eventi con mappatura errata o in alcuni casi che on includono nessun evento.

Configurazione del servizio SAPI Collector

Utilizzare questa procedura per configurare il servizio SAPI Collector.

È possibile modificare i criteri CA Audit che utilizzano azioni di Collector per inviare eventi a un server CA Enterprise Log Manager oltre a, o al posto di, inviare eventi al database CA Audit Collector. Configurare questo servizio prima di modificare i criteri di audit per assicurarsi che non venga perso alcun evento.

Per configurare il servizio SAPI Collector

1. Accedere al server CA Enterprise Log Manager e selezionare la scheda Amministrazione.

   La sottoscheda Raccolta registri verrà visualizzata per impostazione predefinita.

2. Espandere la voce CA Adapters.

3. Selezionare il servizio SAPI Collector.
4. Fare riferimento alla Guida in linea per le descrizioni di ogni campo.
5. Al termine, fare clic su Salva.

Configurazione del servizio SAPI Router

Utilizzare questa procedura per configurare un servizio SAPI Router.

È possibile modificare i criteri CA Audit che utilizzano azioni Route per inviare eventi al server CA Enterprise Log Manager oltre a, o al posto di, eventi di routing verso altre destinazioni. È possibile anche reindirizzare eventi del recorder SAPI affinché raggiungano direttamente il listener del router SAPI modificando i relativi file di configurazione. Configurare questo servizio prima di modificare i criteri di audit o le configurazioni del recorder SAPI per assicurarsi che non venga perso alcun evento.

Per configurare il servizio SAPI Router

1. Accedere al server CA Enterprise Log Manager e selezionare la scheda Amministrazione.

   La sottoscheda Raccolta registri verrà visualizzata per impostazione predefinita.
2. Espandere la voce CA Adapters.
3. Selezionare il servizio SAPI Router.
4. Fare riferimento alla Guida in linea per le descrizioni di ogni campo.
5. Al termina, fare clic su Salva.

Informazioni sul plug-in eventi iTechnology

Il plug-in eventi iTechnology riceve eventi inviati attraverso il meccanismo di gestione eventi iGateway. Configurare il plug-in eventi iTechnology se una delle seguenti affermazioni è vera per l'ambiente in questione:

- Nella rete sono presenti iRecorder che non dispongono di client CA Audit sullo stesso sistema
- Si dispone di altri prodotti, come CA EEM, che possono inoltrare gli eventi attraverso iTechnology

Dopo avere ricevuto un evento, questo servizio lo invia alla libreria del mapping, dopodichè CA Enterprise Log Manager inserisce l'evento mappato nell'archivio registro eventi.

Configurazione del plug-in eventi iTechnology

Utilizzare questa procedura per configurare il plug-in eventi iTechnology per ricevere da iRecorder e altre origini eventi iTechnology.

Utilizzare il plug-in iTechnology quando si configura un iRecorder autonomo per inviare i suoi eventi a un server CA Enterprise Log Manager. Configurare il servizio *prima* di eseguire la configurazione o l'installazione di un iRecorder per verificare che gli eventi non vengano persi.

Nota: se si desidera inviare eventi da un client esterno per il listener del plug-in eventi iTechnology, è necessario inviare tali eventi solo al server CA Enterprise Log Manager secondario.

Per configurare il plug-in eventi iTechnology

1. Accedere al server CA Enterprise Log Manager e selezionare la scheda Amministrazione.

   La sottoscheda Raccolta log verrà visualizzata per impostazione predefinita.

2. Espandere la voce CA Adapters.
3. Selezionare il servizio plug-in eventi iTechnology.
4. Selezionare uno o più file di mapping dei dati (DM) dall'elenco dei file DM disponibili ed utilizzare i pulsanti freccia per spostarli all'elenco di selezione dei file DM.

   Il servizio di plug-in degli eventi è preconfigurato per includere la maggior parte dei principali file di mapping dei dati.

5. Fare clic su Salva per archiviare le modifiche nei file di configurazione del server di gestione.

Invio di eventi CA Audit a CA Enterprise Log Manager

È possibile integrare CA Enterprise Log Manager con l'implementazione CA Audit esistente nei seguenti modi:

- Riconfigurare un iRecorder che non si trova sullo stesso host del client CA Audit per inviare eventi a CA Enterprise Log Manager
- Modificare un criterio CA Audit esistente per inviare eventi sia a CA Audit che a CA Enterprise Log Manager

Configurazione di iRecorder per inviare eventi a CA Enterprise Log Manager

CA Enterprise Log Manager riceve eventi da iRecorder attraverso il listener del plug-in eventi iTech. È necessario configurare il listener prima di modificare la configurazione di iRecorder. Se non viene eseguita questa operazione, i dati degli eventi potrebbero andare perduti. Dopo avere configurato il Listener, utilizzare questa procedura per configurare iRecorder per l'invio di eventi al server CA Enterprise Log Manager.

Gli iRecorder installati sullo stesso computer del client CA Audit inviano eventi direttamente al client. Per queste macchine, è necessario utilizzare gli adapter del raccoglitore o del router SAPI.

Importante: Un iRecorder autonomo può inviare i propri eventi solo ad un'unica destinazione. Se si riconfigura un iRecorder utilizzando la procedura che segue, gli eventi vengono archiviati *solo* nell'archivio registro eventi CA Enterprise Log Manager. Se si devono conservare eventi sia nell'archivio registro eventi che nel database di CA Audit Collector, modificare l'azione di una regola su un criterio esistente o creare un nuovo criterio per un client CA Audit.

Per configurare iRecorder per l'invio di eventi a CA Enterprise Log Manager

1. Accedere al server che ospita iRecorder come utente con privilegi di amministrazione.
2. Navigare fino alla directory del sistema operativo:
   - UNIX o Linux: /opt/CA/SharedComponents/iTechnology
   - Windows: \Program Files\CA\SharedComponents\iTechnology
3. Terminare il daemon o servizio iGateway con il seguente comando:
   - UNIX o Linux: ./S99igateway stop
   - Windows: net stop igateway
4. Modificare il file iControl.conf.
5. Specificare il seguente valore RouteEvent:

   ```
   <RouteEvent>true</RouteEvent>
   ```

   Questa voce indica ad iGateway di inviare i suoi eventi, inclusi tutti gli eventi iRecorder, all'host indicato nella coppia della scheda RouteHost.
6. Specificare il seguente valore RouteHost:

   ```
   <RouteHost>nomehost_CA_ELM</RouteHost>
   ```

   Questa voce indica ad iGateway di inviare i suoi propri eventi al server CA Enterprise Log Manager usando il suo nome DNS.

7. Terminare il daemon o servizio iGateway con il seguente comando:
   - UNIX o Linux: ./S99igateway start
   - Windows: net start igateway

   Questa azione obbliga iRecorder a utilizzare nuove impostazioni e avvia il flusso di eventi da iRecorder al server CA Enterprise Log Manager.

Ulteriori informazioni:

Informazioni su SAPI Router e Collector (a pagina 240)
Configurazione del servizio SAPI Collector (a pagina 241)
Configurazione del servizio SAPI Router (a pagina 242)

Modifica di criteri CA Audit esistenti per inviare eventi a CA Enterprise Log Manager

Utilizzare questa procedura per abilitare un client CA Audit per inviare eventi ad *entrambi* i database di raccolta: di CA Enterprise Log Manager e di CA Audit. Aggiungendo una nuova destinazione alle azioni Route o Collector in una regola esistente, è possibile inviare eventi raccolti ad entrambi i sistemi. In alternativa, è inoltre possibile modificare criteri o regole specifiche per inviare eventi *solo* al server CA Enterprise Log Manager.

CA Enterprise Log Manager raccoglie eventi da client CA Audit utilizzando i listener CA Audit SAPI Router e CA Audit SAPI Collector. Gli eventi raccolti vengono archiviati nell'archivio registro eventi CA Enterprise Log Manager solo *dopo* avere inviato il criterio ai client ed esso diventa attivo.

Importante: è necessario configurare i listener CA Enterprise Log Manager per ricevere eventi prima di modificare e attivare il criterio. Se non si esegue prima questa configurazione, è possibile che gli eventi vengano mappati in modo errato se questi arrivano tra il momento in cui il criterio diventa attivo e quello in cui i listener possono mappare correttamente gli eventi.

Per modificare l'azione della regola di un criterio esistente per inviare gli eventi a CA Enterprise Log Manager

1. Accedere al server gestore dei criteri e accedere alla scheda Criteri personali nel riquadro a sinistra.
2. Espandere la cartella del criterio fino a quando è possibile visualizzare il criterio desiderato.
3. Fare clic sul criterio per visualizzarne le informazioni di base nel riquadro Dettagli a destra.
4. Fare clic su Modifica nel riquadro Dettagli per effettuare aggiunte alle regole del criterio. Viene avviata la procedura guidata della regola.
5. Fare clic su Modifica azioni di fianco alla freccia per il passaggio 3 della procedura guidata. Verrà visualizzata la pagina delle azioni della regola della procedura guidata.
6. Fare clic sull'azione del Collector nel riquadro Sfoglia azioni a sinistra. Questo visualizzerà l'Elenco azioni a destra.

   È anche possibile utilizzare l'azione Route per creare una regola per l'invio degli eventi a un server CA Enterprise Log Manager.
7. Fare clic su Nuova per aggiungere una nuova regola.
8. Immettere l'indirizzo IP o il nome host del server CA Enterprise Log Manager di raccolta.

   Per implementazioni di CA Enterprise Log Manager con due o più server, è possibile immettere un nome host o indirizzo IP CA Enterprise Log Manager diverso nel campo Nome host alternativo per utilizzare la funzionalità di failover automatico di <Aus>. Se il primo server CA Enterprise Log Manager non è disponibile, CA Audit invia automaticamente gli eventi al server indicato nel campo Nome host alternativo.
9. Immettere il nome del server CA Enterprise Log Manager di gestione nel campo Nome host alternativo e creare una descrizione per questa nuova azione della regola.
10. Deselezionare la casella di controllo Esegui questa azione sul server remoto, se selezionata.
11. Fare clic su Aggiungi per salvare la nuova azione della regola e fare clic su Fine nella finestra della procedura guidata.
12. Selezionare la scheda Regole nel riquadro in basso a destra e la regola da selezionare.

13. Fare clic su Controlla criteri per controllare le regole modificate con le nuove azioni per assicurarsi che siano compilate correttamente.

    Eseguire tutte le modifiche necessarie alle regole e assicurarsi che siano compilate correttamente prima di attivarle.

14. Fare clic su Attiva per distribuire i criteri controllati che contengono le nuove azioni della regola aggiunte.
15. Ripetere questa procedura per ogni regola e criterio con eventi raccolti da inviare a CA Enterprise Log Manager.

Ulteriori informazioni:

Informazioni su SAPI Router e Collector (a pagina 240)
Configurazione del servizio SAPI Collector (a pagina 241)
Configurazione del servizio SAPI Router (a pagina 242)

Modifica di un criterio esistente r8SP2 per l'invio di eventi a CA Enterprise Log Manager

Utilizzare questa procedura per abilitare un client CA Audit r8 SP2 per l'invio di eventi ad *entrambi* i database di raccolta: di CA Enterprise Log Manager e di CA Audit. Aggiungendo una nuova destinazione alle azioni Route o Collector in una regola esistente, è possibile inviare eventi raccolti ad entrambi i sistemi. In alternativa, è inoltre possibile modificare criteri o regole specifiche per inviare eventi *solo* al server CA Enterprise Log Manager.

Ulteriori informazioni sul funzionamento dei criteri sono disponibili nella *Guida all'amministrazione CA Audit r8 SP2*. Fare riferimento a questa risorsa per i dettagli sull'esecuzione dei passaggi nella procedura che segue.

CA Enterprise Log Manager raccoglie eventi da client CA Audit utilizzando i listener CA Audit SAPI Router e CA Audit SAPI Collector. Gli eventi raccolti vengono archiviati nell'archivio registro eventi CA Enterprise Log Manager solo *dopo* avere inviato il criterio ai client ed esso diventa attivo.

Importante: è necessario configurare i listener CA Enterprise Log Manager per ricevere eventi prima di modificare e attivare il criterio. Se non si esegue prima questa configurazione, è possibile che gli eventi vengano mappati in modo errato tra il momento in cui il criterio diventa attivo e quello in cui i listener possono mappare correttamente gli eventi.

Per modificare l'azione della regola di un criterio r8 SP2 esistente per inviare gli eventi a CA Enterprise Log Manager

1. Accedere al server del Gestore dei criteri come utente con ruolo di creatore.
2. Accedere alla regola da modificare espandendone la cartella nel riquadro Criteri e selezionando il criterio appropriato.

   Il criterio compare nel riquadro Dettagli, visualizzando le sue regole.
3. Fare clic sulla regola da modificare.

   La regola verrà visualizzata, con le relative azioni, nel riquadro Dettagli.
4. Fare clic su Modifica.

   Viene visualizzata la Modifica guidata della regola.
5. Utilizzare la Modifica guidata della regola per modificare la regola in modo che invii eventi al server CA Enterprise Log Manager in aggiunta o al posto delle destinazioni attuali e fare clic su Fine.
6. Fare clic e applicare il criterio come utente creatore in modo che possa essere approvato da un utente con il ruolo di verificatore.
7. Disconnettersi ed effettuare nuovamente l'accesso al server del Gestore dei criteri come utente con ruolo di verificatore, se l'azienda utilizza la funzionalità di segregazione dei doveri.
8. Rivedere e approvare la cartella dei criteri che contiene il criterio e la regola modificata.

   Dopo che il criterio è stato approvato, il server di distribuzione del Gestore dei criteri stabilisce quando il nuovo criterio viene distribuito ai nodi di controllo. È possibile rivedere il registro di attivazione per controllare lo stato di attivazione di un criterio.
9. Ripetere questa procedura per ogni regola e criterio con eventi raccolti da inviare a CA Enterprise Log Manager.

Quando importare eventi

Se si dispone di un server CA Audit Data Tools esistente con un database Collector, si dispone di una tabella SEOSDATA che contiene i dati degli eventi. Per eseguire i sistemi CA Audit e CA Enterprise Log Manager fianco a fianco e visualizzare rapporti sui dati già raccolti, è possibile importare i dati dalla tabella SEOSDATA.

È possibile eseguire l'utilità di importazione SEOSDATA per eseguire un'importazione dei dati degli eventi dal database di raccolta all'archivio registro eventi CA Enterprise Log Manager. Solitamente, si importano i dati degli eventi subito dopo avere distribuito un server CA Enterprise Log Manager. Se si stanno integrando i due sistemi, è possibile decidere di eseguire l'importazione dei dati più di una volta, a seconda della configurazione dell'utilizzo e della rete.

Nota: l'importazione dei dati dalla tabella SEOSDATA *non* elimina o modifica i dati in essa conservati. La procedura di importazione copia i dati, li analizza ed esegue la loro mappatura nell'archivio registro eventi CA Enterprise Log Manager.

Informazioni sull'utilità di importazione SEOSDATA

L'utilità di importazione LMSeosImport utilizza un'interfaccia da riga di comando e supporta entrambi i sistemi operativi Windows e Solaris. L'utilità esegue le seguenti azioni:

- Si connette alla tabella SEOSDATA per estrarre gli eventi nel modo specificato
- Analizza gli eventi SEOSDATA selezionati in coppie nome-valore
- Invia gli eventi a CA Enterprise Log Manager attraverso lo sponsor eventi SAPI o lo sponsor eventi iTech per l'inserimento nell'archivio registro eventi

Gli eventi vengono mappati nella grammatica evento comune (CEG) che costituisce la base delle tabelle database dell'archivio registro eventi. È possibile quindi utilizzare le query predefinite e i rapporti per raccogliere informazioni dagli eventi archiviati.

Importazione da una tabella SEOSDATA live

L'esecuzione dell'utilità LMSeosImport con una tabella SEOSDATA live è sconsigliata, ma a volte è inevitabile. Se si deve eseguire l'utilità con un database live, essa importerà solo una determinata sezione dei dati. Ciò avviene poiché gli eventi che vengono aggiunti al database *dopo* l'avvio dell'utilità LMSeosImport non vengono importati durante la sessione di importazione.

Ad esempio, se non si specificano i parametri -minid e -maxid nella riga di comando, quando l'utilità viene avviata invia una query al database richiedendo l'entry ID massimo e minimo esistente. L'utilità basa quindi le sue query e importa le attività su tali valori. Gli eventi inseriti nel database dopo l'avvio dell'utilità hanno entry ID all'esterno dell'intervallo e quindi non vengono importati.

Al termine di una sessione di importazione, l'utilità visualizza l'ultimo entry ID elaborato. Potrebbe essere necessario eseguire più di una sessione di importazione per ottenere tutti gli eventi o si può scegliere di attendere per un periodo inferiore di attività di rete e degli eventi prima di eseguire l'utilità di importazione. È possibile eseguire sessioni di importazione aggiuntive, se necessario, utilizzando l'entry ID finale dell'ultima sessione come valore -minid della nuova sessione.

Importazione di dati da una tabella SEOSDATA

Utilizzare questo processo per importare dati da un database di raccolta (tabella SEOSDATA) per garantire i migliori risultati:

1. Copiare l'utilità LMSeosImport nella cartella iTechnology su un server CA Audit Data Tools.

   Nota: l'utilità LMSeosImport richiede le librerie di supporto *etsapi* e *etbase* fornite con il client CA Audit.

2. Nozioni fondamentali della riga di comando e delle opzioni di LMSeosImport.
3. Creare un rapporto di evento per scoprire i tipi di evento e i conteggi, quindi gli intervalli entry ID.
4. Visualizzare l'anteprima dei risultati dell'importazione con i parametri previsti per l'utilizzo.

   È possibile decidere di eseguire nuovamente l'importazione in anteprima per affinare le opzioni della riga di comando, se necessario.

5. Importare gli eventi da un database di raccolta utilizzando le opzioni di riga di comando affinate.

Copia dell'utilità di importazione eventi su un server Solaris Data Tools

Prima di potere importare i dati da una tabella SEOSDATA, è necessario copiare l'utilità LMSeosImport dal DVD-ROM di installazione dell'applicazione CA Enterprise Log Manager sul server Solaris Data Tools.

Nota: l'utilità LMSeosImport richiede la presenza delle librerie *etsapi* ed *etbase*. Questi file fanno parte dell'installazione del server Data Tools di base. Prima di provare a utilizzare l'utilità LMSeosImport, assicurarsi che la directory di installazione di CA Audit sia inclusa nell'istruzione PATH del sistema. La directory predefinita è /opt/CA/eTrustAudit/bin.

Prima di eseguire l'utilità, impostare le seguenti variabili d'ambiente con il comando *env*:

- ODBC_HOME=<*directory di installazione di CA Audit data tools*>/odbc
- ODBCINI=<*directory di installazione di CA Audit data tools*>/odbc/odbc.ini

Per copiare l'utilità

1. Accedere a un prompt dei comandi sul server Solaris Data Tools.
2. Inserire il DVD-ROM di installazione dell'applicazione CA Enterprise Log Manager.
3. Andare alla directory /CA/ELM/Solaris_sparc.
4. Copiare l'utilità LMSeosImport nella directory iTechnology di CA Audit Data Tools /opt/CA/SharedComponents/iTechnology.

   L'utilità è pronta per l'utilizzo dopo averla copiata nella directory designata e dopo avere impostato le variabili d'ambiente necessarie. Non è necessario eseguire un'installazione separata.

Copia dell'utilità di importazione in un server Windows Data Tools

Prima di importare i dati dalla tabella SEOSDATA, è necessario copiare l'utilità LMSeosImport dal DVD-ROM di installazione dell'applicazione CA Enterprise Log Manager al server degli strumenti dati di Windows.

Nota: l'utilità LMSeosImport richiede la presenza delle librerie di collegamento dinamico *etsapi* e *etbase*. Tali file fanno parte dell'installazione di base del server degli strumenti dati. Prima di provare ad utilizzare l'utilità LMSeosImport, assicurarsi che la directory Program Files\CA\eTrust Audit\bin sia inclusa nell'istruzione PATH del sistema.

Per copiare l'utilità

1. Accedere a un prompt dei comandi sul server degli strumenti dati di Windows.
2. Inserire il DVD-ROM di installazione dell'applicazione CA Enterprise Log Manager.
3. Navigare alla directory \CA\ELM\Windows.
4. Copiare l'utilità LMSeosImport.exe nella directory iTechnology del server degli strumenti dati CA Audit, <drive>:\Program Files\CA\SharedComponents\iTechnology.

   L'utilità è pronta per l'utilizzo dopo averla copiata nella directory designata. Non è necessario eseguire un'installazione separata.

Nozioni fondamentali sulla riga di comando di LMSeosImport

L'utilità LMSeosImport offre una serie di argomenti da riga di comando che permettono di controllare quali eventi vengono trasferiti. Ogni evento nella tabella SEOSDATA è una riga a sé stante e dispone di un *entry ID* per identificarlo. È possibile utilizzare l'utilità di importazione per recuperare un rapporto che elenca molti tipi diversi di informazioni utili. Il rapporto elenca il numero di eventi nella tabella SEOSDATA (come il numero di entry ID), il conteggio degli eventi per tipo di registro e gli intervalli delle date degli eventi. L'utilità offre un'opzione per riprovare in caso si verifichi un errore durante l'importazione di un evento.

È anche possibile eseguire un lavoro in anteprima per visualizzare quali sarebbero i risultati dell'importazione con una struttura di comando specifica. I lavori in anteprima non importano realmente i dati, ma permettono di affinare le opzioni di riga di comando prima dello spostamento attuale.

È possibile eseguire l'utilità di migrazione più di una volta utilizzando parametri diversi per importare tipi diversi di dati. Ad esempio, è possibile scegliere di trasferire i propri dati in diverse sessioni su misura in base a un intervallo di entry ID, al tipo di registro o a intervalli di date specifiche.

Nota: l'utilità *non* offre il tracciamento delle importazioni delle sessioni precedenti. È possibile duplicare i dati nel database CA Enterprise Log Manager se si esegue il comando con gli stessi parametri più di una volta.

Per risultati migliori, suddividere l'importazione per tipo di registro (utilizzando l'opzione -log) o per entry ID (utilizzando le opzioni -minid e -maxid) per migliorarne le prestazioni. Utilizzare l'opzione -retry per assicurare il ripristino da errori che si potrebbero verificare durante l'importazione di eventi. L'utilità utilizza un valore -retry predefinito di 300 secondi per massimizzare la riuscita dell'importazione.

Comandi e opzioni dell'utilità di importazione

L'utilità LMSeosImport supporta la seguente sintassi della riga di comando e le seguenti opzioni:

```
LMSeosImport -dsn nome_dsn -user nome_utente -password password -target
nome_destinazione {-sid nnn -eid nnnn -stm aaaa-mm-gg -etm aaaa-mm-gg -log
nomeaccesso -transport (sapi|itech) -chunk nnnn -pretend -verbose -delay -report
-retry}
```

-dsn

Specifica il nome del server host in cui risiede la tabella SEOSDATA. Questo parametro è obbligatorio.

-user

Specifica un identificativo utente valido che abbia almeno accesso in lettura alla tabella SEOSDATA. Questo parametro è obbligatorio.

-password

Consente di specificare la password per l'account utente specificato con il parametro -user. Questo parametro è obbligatorio.

-target

Specifica il nome host o l'indirizzo IP del server CA Enterprise Log Manager per ricevere gli eventi migrati dalla tabella SEOSDATA. Questo parametro è obbligatorio.

-minid nnnn

Indica l'ENTRYID iniziale utilizzato nella selezione degli eventi dalla tabella SEOSDATA. Questo parametro è facoltativo.

-maxid nnnn

Indica l'ENTRYID finale utilizzato nella selezione degli eventi dalla tabella SEOSDATA. Questo parametro è facoltativo.

-mintm AAAA-MM-GG

Indica l'ora di inizio (in formato AAAA-MM-GG) utilizzata nella selezione degli eventi dalla tabella SEOSDATA. Questo parametro è facoltativo.

-maxtm AAAA-MM-GG

Indica l'ora di fine (in formato AAAA-MM-GG) utilizzata nella selezione degli eventi dalla tabella SEOSDATA. Questo parametro è facoltativo.

-log logname

Consente di specificare, da parte dell'utilità, la selezione dei soli rapporti di eventi con questo nome log specificato. Questo parametro è facoltativo. Se il nome del registro contiene spazi, deve essere incluso in virgolette doppie.

-transport <sapi | itech >

Specifica il metodo di trasporto che deve essere utilizzato tra l'utilità di importazione e CA Enterprise Log Manager. Il metodo di trasporto predefinito è sapi.

-chunk nnnn

Consente di specificare il numero di rapporti di eventi da selezionare dalla tabella SEOSDATA in ogni passaggio. Il valore predefinito è 5000 eventi (righe). Questo parametro è facoltativo.

-preview

Esegue l'output dei risultati delle selezioni dei record eventi in STDOUT, ma non importa realmente i dati. Questo parametro è facoltativo.

-port

Consente di specificare il numero di porta da utilizzare se è stata impostata l'opzione di trasporto per SAPI ed è stato configurato il router SAPI di CA Enterprise Log Manager per l'utilizzo di un valore di porta fisso (senza utilizzare il portmapper).

-verbose

Specifica che l'utilità invia messaggi di elaborazione dettagliati a STDOUT. Questo parametro è facoltativo.

-delay

Specifica il numero di secondi di pausa tra l'elaborazione di ogni evento. Questo parametro è facoltativo.

-report

Consente di visualizzare un rapporto di intervallo di tempo, ENTRYID, e i conteggi di log nella tabella SEOSDATA. Questo parametro è facoltativo.

-retry

Consente di specificare il numero di secondi durante i quali vengono effettuati nuovi tentativi ogni volta che si verifica un errore durante l'importazione di un evento. L'elaborazione continua quando l'invio di tale evento viene eseguito di nuovo correttamente. L'utilità utilizza automaticamente un valore predefinito di 300 secondi. Non è necessario immettere il parametro a meno che non si voglia specificare un valore diverso. I messaggi relativi allo stato dei nuovi tentativi vengono inviati a STDOUT.

Esempi di riga di comando di LMSeosImport

È possibile utilizzare i seguenti esempi di riga di comando per creare un comando personalizzato quando si utilizza l'utilità di importazione SEOSDATA.

Per eseguire un'importazione di registrazioni tra ENTRYID 1000 e 4000

Inserire il seguente comando:

```
LMSeosImport –dsn eAudit_DSN –user sa –password sa –target 130.200.137.192 –
minid 1000 –maxid 4000
```

Per eseguire un'importazione di registrazioni solo per eventi di applicazioni NT

Inserire il seguente comando:

```
LMSeosImport –dsn eAudit_DSN –user sa –password sa –target 130.200.137.192 –
log NT-Application
```

Creazione di un evento di rapporto

L'esecuzione di un evento di rapporto SEOSDATA prima dell'importazione dei dati effettiva fornisce le informazioni necessarie sugli eventi nella tabella. Il rapporto mostra l'intervallo di tempo dell'evento, il conteggio eventi per tipo di registro e l'intervallo entry ID. È possibile utilizzare i valori visualizzati nel rapporto per perfezionare le opzioni della riga di comando per un comando di anteprima o per il comando di importazione effettivo.

Per visualizzare un rapporto delle informazioni dell'evento SEOSDATA corrente in Windows

1. Accedere a un prompt dei comandi sul server CA Audit Data Tools.
2. Andare alla directory \Program Files\CA\SharedComponents\iTechnology.
3. Inserire il seguente comando:

```
LMSeosImport –dsn eAudit_DSN –user sa –password sa -target
<nome_host_Log_Manager> –report
```

La visualizzazione del rapporto generato è simile al seguente esempio:

```
SEOSProcessor::InitOdbc: successfully attached to source [eAudit_DSN]

---------- SEOSDATA Event Time Range ----------

Minimum TIME = 2007-08-27
Maximum TIME = 2007-10-06

---------- Event Count Per Log ----------

com.ca.iTechnology.iSponsor : 3052
EiamSdk : 1013
NT-Application : 776
NT-System : 900

---------- SEOSDATA EntryID Range ----------

Minimum ENTRYID : 1
Maximum ENTRYID : 5741

Report Completed.
```

Anteprima dei risultati dell'importazione

È possibile eseguire un'importazione di prova con output in STDOUT per visualizzare in anteprima i risultati dell'importazione senza importare o trasferire realmente i dati. Si tratta di un buon metodo per provare i parametri della riga di comando immessi per un trasferimento singolo o per un'importazione in batch che si verifica regolarmente.

Per eseguire un'importazione di prova al fine di visualizzare in anteprima i risultati dell'importazione

1. Accedere a un prompt dei comandi sul server CA Audit Data Tools.
2. Passare alla seguente directory:

   Solaris: /opt/CA/SharedComponents/iTechnology

   Windows: \Program Files\CA\SharedComponents\iTechnology
3. Inserire il seguente comando:

   Per Solaris:

   ```
   ./LMSeosImport.sh –dsn eAudit_DSN –user sa –password sa –target
   <nome_o_IP_host_Log_Manager> –minid 1000 –maxid 4000 -preview
   ```

   Per Windows:

   ```
   LMSeosImport.exe –dsn eAudit_DSN –user sa –password sa –target
   <nome_o_IP_host_Log_Manager> –minid 1000 –maxid 4000 -preview
   ```

Importazione di eventi da un database Windows Collector

È possibile utilizzare questa procedura per importare dati degli eventi da un database Collector che risiede su un server Windows Data Tools.

Per importare eventi da una tabella SEOSDATA in un server Windows

1. Individuare il nome del server su cui si trova la tabella SEOSDATA.
2. Assicurarsi di disporre di credenziali di accesso al server con almeno accesso in lettura alla tabella SEOSDATA.
3. Accedere a un prompt dei comandi sul server CA Audit Data Tools.
4. Andare alla directory \Program Files\CA\Shared Components\iTechnology.
5. Avviare l'utilità di importazione utilizzando la sintassi del comando:

   ```
   LMSeosImport.exe -dsn <nomedsn> -user <UID> -password <password> -target
   <nomehostdestinazione> <flag opzionali>
   ```

Importazione di eventi da un database Solaris Collector

È possibile utilizzare questa procedura per importare dati degli eventi da un database Collector che risiede su un server Solaris Data Tools.

Per importare eventi da una tabella SEOSDATA in un server Solaris

1. Individuare il nome del server su cui si trova la tabella SEOSDATA.
2. Assicurarsi di disporre di credenziali di accesso al server con almeno accesso in lettura alla tabella SEOSDATA.
3. Accedere a un prompt dei comandi sul server CA Audit Data Tools.
4. Andare alla directory /opt/CA/SharedComponents/iTechnology.
5. Avviare l'utilità di importazione utilizzando la sintassi del comando:

```
./LMSeosImport -dsn <nomedsn> -user <UID> -password <password> -target
<nomehostdestinazione> <flag opzionali>
```

Appendice B: Considerazioni per gli utenti CA Access Control

Questa sezione contiene i seguenti argomenti:

Integrazione con CA Access Control

È possibile integrare CA Enterprise Log Manager con CA Access Control utilizzando uno di molti livelli di versioni diverse. L'approccio generale è il seguente:

Per le versioni CA Access Control che utilizzano un server di messaggi TIBCO per il routing di eventi, procedere come segue:

- Installare un agente CA Enterprise Log Manager.
- Configurare un connettore che utilizzi il connettore AccessControl_R12SP1_TIBCO_Connector

Per CA Access Control r12.5, consultare la *Guida all'implementazione di CA Access Control r12.5* e la *Guida ai connettori CA Enterprise Log Manager CA Access Control*.

Per CA Access Control r12. SP1, consultare la terza edizione della *Guida all'implementazione di CA Access Control r12 SP1* e la *Guida ai connettori CA Enterprise Log Manager per CA Access Control*.

Nota: queste implementazioni usano i componenti che fanno parte delle CA Access Control Premium Edition.

Per le versioni di CA Access Control che utilizzano selogrd per il routing di eventi, procedere come segue:

- Installare un agente CA Enterprise Log Manager.
- Configurare in connettore che utilizzi l'integrazione ACSelogrd

Ulteriori informazioni sulla configurazione di un connettore per la raccolta di eventi CA Access Control sono disponibili nella *Guida ai connettori per CA Access Control r8 SP1*.

Se attualmente si inviano gli eventi CA Access Control a CA Audit, utilizzare i seguenti metodi per ricevere gli eventi inCA Enterprise Log Manager:

- Modifica di un criterio CA Audit esistente per inviare eventi sia a CA Audit che a CA Enterprise Log Manager, se si utilizza un iRecorder CA Audit per raccogliere eventi. È inoltre possibile modificare il criterio per inviare eventi solo al server CA Enterprise Log Manager, se lo si desidera.
- Configurare il file control.conf in modo che l'iRecorder invii gli eventi direttamente a CA Enterprise Log Manager.

Nota: se si dispone di una versione di eTrust Access Control che non supporta iRecorder, è possibile inviare eventi direttamente al router CA Audit. Fare riferimento alle informazioni sull'integrazione di CA Audit nella *Guida all'amministrazione di eTrust Access Control r5.3* per ulteriori informazioni.

Le seguenti linee guida utilizzano la serie r8 SP2 per l'interfaccia utente dello strumento di gestione dei criteri. Le procedure generali sono le stesse delle versione di CA Audit precedenti, nonostante l'interfaccia utente sia diversa.

Come modificare criteri di CA Audit per l'invio di eventi a CA Enterprise Log Manager

La procedura per la modifica di un criterio CA Audit esistente per l'invio di eventi a CA Enterprise Log Manager implica i seguenti passaggi:

- Raccogliere le informazioni necessarie:
  - Assicurarsi di disporre delle credenziali utente per Gestione criteri di CA Audit con l'autorizzazione per creare, selezionare e attivare i criteri.
  - Ottenere l'indirizzo IP o il nome host necessario per accedere all'interfaccia utente di Audit Administrator. L'URL di accesso alle applicazioni Web di Gestione criteri delle serie r8 SP2 ha il seguente formato:

    `https://<indirizzo_IP_di_CA Audit_PM>:5250/spin/auditadmin`

- Configurare il servizio collector SAPI o router SAPI CA Enterprise Log Manager, a seconda di come si intende creare l'azione della nuova regola.

  Se si ha intenzione di creare un'azione Collector, configurare il collector SAPI. Se si ha intenzione di configurare un'azione Route, configurare il router SAPI.

  Nota: l'esempio in questa sezione utilizza l'azione Collector.

- Localizzare e modificare un criterio esistente CA Access Control per inviare gli eventi a CA Enterprise Log Manager.
- Selezionare e attivare il criterio modificato per distribuirlo ai nodi di audit.

Ripetere questa procedura per aggiungere azioni della nuova regola ad altre regole del criterio, a seconda delle esigenze.

Ulteriori informazioni:

Informazioni su SAPI Router e Collector (a pagina 240)

Configurazione di SAPI Collector Adapter per la ricezione di eventi di CA Access Control

utilizzare questa procedura per configurare SAPI Collector Adapter per ricevere eventi di CA Access Control da un'implementazione di CA Audit.

È possibile modificare i criteri CA Audit che utilizzano azioni di Collector per inviare eventi a un server CA Enterprise Log Manager oltre a, o al posto di, inviare eventi al database CA Audit Collector. Configurare il servizio *prima* di modificare i criteri di CA Audit accertandosi che non vadano persi degli eventi.

Il servizio router SAPI può essere configurato in modo simile. Se si utilizzano entrambi i servizi Router e Collector, assicurarsi che le porte elencate siano diverse o che siano controllate dal servizio PortMapper.

Per configurare il servizio SAPI Collector

1. Accedere al server CA Enterprise Log Manager come utente Amministratore e selezionare la scheda Amministrazione.

   La sottoscheda Raccolta registri verrà visualizzata per impostazione predefinita.

2. Espandere la voce CA Adapters.



3. Selezionare il servizio SAPI Collector

4. Selezionare la casella di controllo Abilita listener e impostare il valore SapiPort su un valore corrispondente a quello utilizzato da CA Audit.

   Il valore CA Enterprise Log Manager predefinito, 0, utilizza il servizio PortMapper per la mappatura delle porte. Se in CA Audit è stata definita una porta, usare tale impostazione in questo punto.

5. Accettare i valori predefiniti degli altri campi e scorrere verso il basso nell elenco File di mapping.

   Se si seleziona la casella di controllo Registra, specificare il valore di una porta SAPI.

6. Aggiungere la voce del file di mapping Access Control se non è presente ed eliminare le altre selezioni dei file di mapping dall'elenco dei file di mapping selezionati.

7. Fare clic su Salva.

Modifica di criteri CA Audit esistenti per inviare eventi a CA Enterprise Log Manager

Utilizzare questa procedura per abilitare un client CA Audit per inviare eventi ad *entrambi* i database di raccolta: di CA Enterprise Log Manager e di CA Audit. Aggiungendo una nuova destinazione alle azioni Route o Collector in una regola esistente, è possibile inviare eventi raccolti ad entrambi i sistemi. In alternativa, è inoltre possibile modificare criteri o regole specifiche per inviare eventi *solo* al server CA Enterprise Log Manager.

CA Enterprise Log Manager raccoglie eventi da client CA Audit utilizzando i listener CA Audit SAPI Router e CA Audit SAPI Collector. CA Enterprise Log Manager può inoltre raccogliere gli eventi usando il plug-in iTech direttamente se gli iRecorder sono configurati per l'invio diretto al server CA Enterprise Log Manager. Gli eventi raccolti vengono archiviati nell'archivio di registro eventi CA Enterprise Log Manager solo *dopo* aver inviato il criterio ai client e una volta che questo è diventato attivo.

Importante: è necessario configurare i listener CA Enterprise Log Manager per la ricezione di eventi prima di modificare e attivare il criterio. Se non si esegue prima questa configurazione, è possibile che gli eventi vengano mappati in modo errato tra il momento in cui il criterio diventa attivo e quello in cui i listener possono mappare correttamente gli eventi.

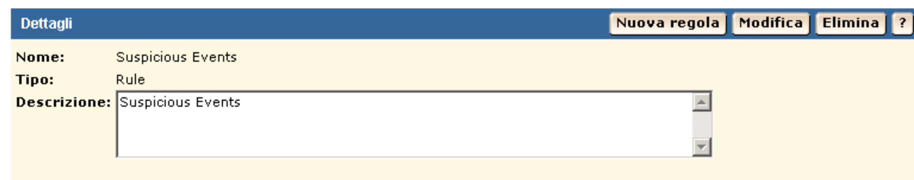
Per modificare l'azione della regola di un criterio esistente per l'invio di eventi a CA Enterprise Log Manager

1. Accedere al server gestore dei criteri e accedere alla scheda Criteri personali nel riquadro a sinistra.

2. Espandere la cartella del criterio fino a quando è possibile visualizzare il criterio desiderato.

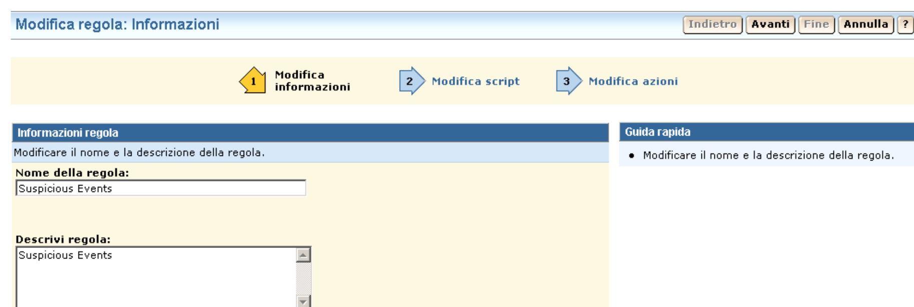


3. Fare clic sul criterio per visualizzarne le informazioni di base nel riquadro Dettagli a destra.



4. Fare clic su Modifica nel riquadro Dettagli per effettuare aggiunte alle regole del criterio.

   Viene avviata la procedura guidata della regola:



5. Fare clic su Modifica azioni di fianco alla freccia per il passaggio 3.

   Verrà visualizzata la pagina delle azioni della regola:

6. Fare clic sull'azione collector nel riquadro Sfoglia azioni per visualizzare l'elenco delle azioni sulla destra.

   È inoltre possibile utilizzare l'azione di routing, ma l'azione collector offre il vantaggio aggiuntivo di un nome host alternativo per l'elaborazione di failover di base..

7. Fare clic su Nuova per aggiungere una nuova regola.

8. Immettere l'indirizzo IP o il nome host del server CA Enterprise Log Manager di raccolta.

   Nel caso di un'implementazione CA Enterprise Log Manager con due o più server, è possibile inserire un nome host CA Enterprise Log Manager diverso o un indirizzo IP nel campo Nome host alternativo. In questo modo si utilizza la funzione di failover automatica di CA Audit. Se il primo server CA Enterprise Log Manager non è disponibile, CA Audit invia automaticamente gli eventi al server indicato nel campo Nome host alternativo.

9. Immettere il nome del server CA Enterprise Log Manager di gestione nel campo Nome host alternativo e creare una descrizione per questa nuova azione della regola.

10. Deselezionare la casella di controllo Esegui questa azione sul server remoto, se selezionata.

11. Fare clic su Aggiungi per salvare la nuova azione della regola e fare clic su Fine nella finestra della procedura guidata.

    Nota: successivamente si dovrà selezionare e attivare il criterio, quindi *non* disconnettersi da Gestione criteri di CA Audit.

Ulteriori informazioni:

Modifica di un criterio esistente r8SP2 per l'invio di eventi a CA Enterprise Log Manager (a pagina 247)

Selezionare e attivare il Criterio modificato

Dopo avere modificato un criterio esistente per aggiungere l'azione di una regola, selezionarlo (compilarlo) e attivarlo.

Per selezionare e attivare un criterio di CA Access Control

1. Selezionare la scheda Regole nel riquadro in basso a destra e la regola da selezionare.



2. fare clic su Controlla criteri per controllare le regole modificate con le nuove azioni per assicurarsi che siano compilate correttamente.

   Eseguire tutte le modifiche necessarie alle regole e assicurarsi che siano compilate correttamente prima di attivarle.

3. Fare clic su Attiva per distribuire i criteri controllati che contengono le nuove azioni della regola aggiunte.

4. Ripetere questa procedura per ogni regola e criterio con eventi raccolti da inviare a CA Enterprise Log Manager.

Configurazione di un iRecorder CA Access Control per l'invio di eventi a CA Enterprise Log Manager

È possibile configurare un iRecorder CA Access Control autonomo per fare in modo che invii gli eventi raccolti direttamente al server CA Enterprise Log Manager per l'archiviazione e la creazione di rapporti. La procedura include i seguenti passaggi:

1. Configurare il listener del plug-in eventi iTech per la ricezione di informazioni da un iRecorder CA Access Control.
2. Scaricare e installare un iRecorder CA Access Control.
3. Configurare l'iRecorder per l'invio diretto degli eventi raccolti a CA Enterprise Log Manager
4. Verificare che CA Enterprise Log Manager stia ricevendo eventi.

Nota: un iRecorder può inviare i propri eventi verso un'unica destinazione. Quando si esegue la configurazione utilizzando questa procedura, l'unica destinazione sarà il server CA Enterprise Log Manager indicato.

Configurazione del plug-in eventi iTech per gli eventi CA Access Control

Prima di riconfigurare un iRecorder per l'invio di eventi direttamente a CA Enterprise Log Manager, è necessario configurare un listener per ricevere tali eventi.

Per configurare il listener

1. Accedere al server CA Enterprise Log Manager come utente con ruolo di amministratore.
2. Accedere alla scheda Amministrazione ed espandere il nodo Adapter CA.



3. Espandere il nodo del plug-in eventi iTechnology.
4. Selezionare il server CA Enterprise Log Manager corrente per visualizzare le impostazioni locali.
5. Assicurarsi che il file di mapping di AccessControl sia il primo dell'elenco dei file di mapping selezionati per garantire il funzionamento più efficiente possibile.
6. Verificare che il valore Livello registro sia impostato su NOTSET per raccogliere tutti i livelli degli eventi.
7. Fare clic su Salva.

Download e installazione di un iRecorder di CA Access Control

È possibile raccogliere eventi di CA Access Control per l'invio a un server CA Enterprise Log Manager anche se CA Audit non è installato. Quando si raccolgono eventi in questo modo, si sta utilizzando un iRecorder in modalità autonoma. È possibile ottenere un iRecorder dal sito web del supporto di CA.

Nota: gli iRecorder sono supportati solo con CA Access Control r8 e versioni successive.

Per scaricare e installare un iRecorder

1. Accedere al seguente sito web di CA:

   `https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/154/cacirecr8-certmatrix.html#caacirec`

2. Selezionare un iRecorder appropriato per la propria versione di CA Access Control.
3. Visualizzare e seguire le istruzioni di installazione disponibili dal collegamento Guida di integrazione nella matrice.

Configurazione di un iRecorder CA Access Control autonomo

Utilizzare questa procedura per configurare l'iRecorder per l'invio di eventi CA Access Control a CA Enterprise Log Manager.

Importante: Un iRecorder autonomo può inviare i propri eventi solo ad un'unica destinazione. Se si configura un iRecorder utilizzando la procedura seguente, tutti gli iRecorder installati su questo sistema invieranno i loro eventi *solo* all'archivio registro eventi CA Enterprise Log Manager indicato.

Gli iRecorder installati sullo stesso computer del client CA Audit inviano eventi direttamente al client. Per questi server, è necessario modificare un criterio CA Audit esistente per aggiungere azioni delle regole e in seguito configurare gli adapter del raccoglitore o del router SAPI di CA Enterprise Log Manager.

Per configurare iRecorder per l'invio di eventi a CA Enterprise Log Manager

1. Accedere al server che ospita iRecorder come utente con privilegi di amministrazione o principale.
2. Navigare fino alla directory del sistema operativo:
   - UNIX o Linux: /opt/CA/SharedComponents/iTechnology
   - Windows: \Program Files\CA\SharedComponents\iTechnology

3. Terminare il daemon o servizio iGateway con il seguente comando:
   - UNIX o Linux: ./S99igateway stop
   - Windows: net stop igateway
4. Modificare il file iControl.conf.

   A seguire un file iControl campione con le sezioni necessarie per modificare in grassetto:

```
<?xml version='1.0' encoding='UTF-8' standalone='no'?>
<iSponsor>
    <Name>iControl</Name>
    <ImageName>iControl</ImageName>
    <Version>4.5.0.2</Version>
    <DispatchEP>iDispatch</DispatchEP>
    <ISType>DSP</ISType>
    <Gated>false</Gated>
    <PreLoad>true</PreLoad>
    <RouteEvent>false</RouteEvent>
    <RouteEventHost>localhost</RouteEventHost>
    <EventsToCache>100</EventsToCache>
    <EventUseHttps>true</EventUseHttps>
    <EventUsePersistentConnections>true</EventUsePersistentConnections>
    <EventUsePipeline>false</EventUsePipeline>
    <StoreEventHost max="10000">localhost</StoreEventHost>
    <RetrieveEventHost interval="60">localhost</RetrieveEventHost>
    <UID>ef1f44ef-r8sp1cr3596a1052-abcd28-2</UID>
    <PublicKey>Valore_Chiave_Pubblica</PublicKey>
    <PrivateKey>Valore_Chiave_Privata</PrivateKey>
    <EventsToQueue>10</EventsToQueue>
</iSponsor>
```

5. Specificare il seguente valore RouteEvent:

```
<RouteEvent>true</RouteEvent>
```

   Questa voce indica ad iGateway di inviare i suoi eventi, inclusi tutti gli eventi iRecorder, all'host indicato nella coppia della scheda RouteEventHost.

6. Specificare il seguente valore RouteEventHost:

```
<RouteEventHost>Nomehost_CA_Enterprise_Log_Manager</RouteEventHost>
```

   Questa voce indica ad iGateway di inviare i suoi propri eventi al server CA Enterprise Log Manager usando il suo nome DNS.

7. Salvare e chiudere il file.
8. Terminare il daemon o servizio iGateway con il seguente comando:
   - UNIX o Linux: ./S99igateway start
   - Windows: net start igateway

   Questa azione obbliga iRecorder a utilizzare nuove impostazioni e avvia il flusso di eventi da iRecorder al server CA Enterprise Log Manager.

Importazione di eventi CA Access Control da un database di raccolta CA Audit

La procedura per l'impostazione di eventi CA Access Control da una tabella SEOSDATA include quanto segue:

1. Copia dell'utilità LMSeosImport nel server CA Audit Data Tools.
2. Creazione di un rapporto di evento per stabilire se gli eventi CA Access Control sono presenti all'interno del database.
3. Esecuzione di un'anteprima dell'importazione con parametri specifici di CA Access Control.
4. Importazione degli eventi di CA Access Control.
5. Esecuzione di query e rapporti CA Enterprise Log Manager sugli eventi importati.

Prerequisiti per l'importazione di eventi CA Access Control

Prima di utilizzare l'utilità LMSeosImport, eseguire quanto segue:

- Ottenere un account utente di database con almeno accesso IN LETTURA alla tabella SEOSDATA CA Audit
- Copiare l'utilità LMSeosImport nel server CA Audit Data Tools
- Accedere a un prompt dei comandi nel server Data Tools e navigare alla directory appropriata:

  Solaris: /opt/CA/SharedComponents/iTechnology

  Windows: \Program Files\CA\SharedComponents\iTechnology

Copia dell'utilità di importazione in un server Windows Data Tools

Prima di importare i dati dalla tabella SEOSDATA, è necessario copiare l'utilità LMSeosImport dal DVD-ROM di installazione dell'applicazione CA Enterprise Log Manager al server degli strumenti dati di Windows.

Nota: l'utilità LMSeosImport richiede la presenza delle librerie di collegamento dinamico *etsapi* e *etbase*. Tali file fanno parte dell'installazione di base del server degli strumenti dati. Prima di provare ad utilizzare l'utilità LMSeosImport, assicurarsi che la directory Program Files\CA\eTrust Audit\bin sia inclusa nell'istruzione PATH del sistema.

Per copiare l'utilità

1. Accedere a un prompt dei comandi sul server degli strumenti dati di Windows.
2. Inserire il DVD-ROM di installazione dell'applicazione CA Enterprise Log Manager.
3. Navigare alla directory \CA\ELM\Windows.
4. Copiare l'utilità LMSeosImport.exe nella directory iTechnology del server degli strumenti dati CA Audit, <drive>:\Program Files\CA\SharedComponents\iTechnology.

   L'utilità è pronta per l'utilizzo dopo averla copiata nella directory designata. Non è necessario eseguire un'installazione separata.

Copia dell'utilità di importazione eventi su un server Solaris Data Tools

Prima di potere importare i dati da una tabella SEOSDATA, è necessario copiare l'utilità LMSeosImport dal DVD-ROM di installazione dell'applicazione CA Enterprise Log Manager sul server Solaris Data Tools.

Nota: l'utilità LMSeosImport richiede la presenza delle librerie *etsapi* ed *etbase*. Questi file fanno parte dell'installazione del server Data Tools di base. Prima di provare a utilizzare l'utilità LMSeosImport, assicurarsi che la directory di installazione di CA Audit sia inclusa nell'istruzione PATH del sistema. La directory predefinita è /opt/CA/eTrustAudit/bin.

Prima di eseguire l'utilità, impostare le seguenti variabili d'ambiente con il comando *env*:

- ODBC_HOME=<*directory di installazione di CA Audit data tools*>/odbc
- ODBCINI=<*directory di installazione di CA Audit data tools*>/odbc/odbc.ini

Per copiare l'utilità

1. Accedere a un prompt dei comandi sul server Solaris Data Tools.
2. Inserire il DVD-ROM di installazione dell'applicazione CA Enterprise Log Manager.
3. Andare alla directory /CA/ELM/Solaris_sparc.
4. Copiare l'utilità LMSeosImport nella directory iTechnology di CA Audit Data Tools /opt/CA/SharedComponents/iTechnology.

   L'utilità è pronta per l'utilizzo dopo averla copiata nella directory designata e dopo avere impostato le variabili d'ambiente necessarie. Non è necessario eseguire un'installazione separata.

Creazione di un rapporto eventi SEOSDATA per eventi CA Access Control

Per stabilire se una tabella SEOSDATA esistente contiene eventi CA Access Controle per decidere sull'importazione di un metodo, è necessario eseguire un rapporto eventi. Il nome di accesso per gli eventi di CA Access Control è *eTrust Access Control*. Il rapporto elenca tutti gli eventi all'interno del database separati dai loro nomi di registro. Il modo più semplice importare eventi di CA Access Control, è importarli in base al loro nome di registro.

Per creare un rapporto di evento

1. Creare un rapporto di evento in modo che sia possibile visualizzare quali eventi di CA Access Control sono presenti nella tabella SEOSDATA.

   ```
   LMSeosImport –dsn My_Audit_DSN –user sa –password sa –report
   ```

   Dopo l'elaborazione, l'utilità visualizza un rapporto che assomiglia al seguente:

   ```
   Import started on Fri Jan  2 15:20:30 2009


   No transport specified, defaulting to SAPI...

   Preparing ODBC connections...

   Successfully attached to source [My_Audit_DSN]

   ---------- SEOSDATA Event Time Range ----------

   Minimum TIME = 2008-05-27
   Maximum TIME = 2009-01-02

   ---------- Event Count Per Log ----------

   Unix : 12804
   ACF2 : 1483
   eTrust AC : 143762
   com.ca.iTechnology.iSponsor : 66456
   NT-Application : 5270
   CISCO PIX Firewall : 5329
   MS IIS : 6765
   Netscape : 530
   RACF : 14
   Apache : 401
   N/A : 28222
   SNMP-recorder : 456
   Check Point FW-1 : 1057
   EiamSdk : 2790
   MS ISA : 609
   ORACLE : 2742
   eTrust PCM : 247
   NT-System : 680
   eTrust Audit : 513
   NT-Security : 14714
   CISCO Device : 41436
   SNORT : 1089

   ---------- SEOSDATA EntryID Range ----------
   ```

```
Minimum ENTRYID : 1
Maximum ENTRYID : 10000010243


Report Completed.

Successfully detached from source [My_Audit_DSN]

Exiting Import....
```

2. Rivedere il rapporto per assicurarsi che gli eventi da CA Access Control siano presenti.

   La riga in grassetto in questa sezione di rapporto mostra che sono presenti eventi di CA Access Control contenuti in questa tabella SEOSDATA.

```
---------- Event Count Per Log ----------

Unix : 12804
ACF2 : 1483
eTrust AC : 143762
com.ca.iTechnology.iSponsor : 66456
NT-Application : 5270
...
```

Anteprima di un rapporto di eventi di CA Access Control

È possibile visualizzare l'anteprima dell'importazione per ottimizzare i parametri di importazione. Questo esempio dimostra due passaggi di anteprima, basati sull'esigenza di importare eventi da un periodo di tempo specifico. L'esempio dà per scontati questi due elementi:

- Il server Data Tools CA Audit risiede in un computer Windows.
- Il nome del database per la tabella SEOSDATA è My_Audit_DSN.
- Il nome utente del database è sa con password sa.
- L'anteprima di importazione utilizza solo il nome di accesso come criteri di ricerca e di importazione.

L'output del comando con opzione -preview invia risultati campione dell'importazione a STDOUT (questo esempio utilizza il valore *My_CA-ELM_Server* per rappresentare un nome del server CA Enterprise Log Manager).

Per visualizzare l'anteprima dell'importazione

1. Visualizzare in anteprima l'importazione dell'evento CA Access Control con il seguente comando:

   ```
   LMSeosImport.exe –dsn My_Audit_DSN –user sa –password sa -target My_CA-ELM_Server –log "eTrust Access Control" -preview
   ```

   Il comando -preview mostra informazioni come le seguenti:

   ```
   Import started on Fri Jan  2 15:35:37 2009


   No transport specified, defaulting to SAPI...

   Preparing ODBC connections...

   Successfully attached to source [My_Audit_DSN]

   No starting ENTRYID specified, using minimum ENTRYID of 1...

   Import (preview) running, please wait...

   .........

   Import (preview) Completed (143762 records in 4 minutes 12 seconds).

   ---------- Imported Events (preview) By Log ----------

   eTrust AC :     143762

   Last EntryId processed: 101234500

   Successfully detached from source [My_Audit_DSN]

   Exiting Import...
   ```

   Per visualizzare in anteprima i risultati, notare che è presente un numero abbastanza ampio di eventi CA Access Control da importare. Supponiamo per questo esempio che sia necessario importare solamente gli eventi verificatisi in un periodo di due mesi. È possibile adattare il comando di anteprima per importare un gruppo più piccolo di eventi in base alla data.

2. Modificare i parametri di importazione per includere un intervallo di date ed eseguire nuovamente l'anteprima con il seguente comando:

```
LMSeosImport.exe –dsn My_Audit_DSN –user sa –password sa -target My_CA-ELM_Server –log "eTrust Access Control" -mintm 2008-11-01 -maxtm 2009-12-31 -preview
```

Il comando amended mostra informazioni come le seguenti:

```
Import started on Fri Jan  2 15:41:23 2009


No transport specified, defaulting to SAPI...

Preparing ODBC connections...

Successfully attached to source [My_Audit_DSN]

No starting ENTRYID specified, using minimum ENTRYID of 1...

Import (preview) running, please wait...

.........

Import (preview) Completed (143762 records in 4 minutes 37 seconds).

---------- Imported Events (preview) By Log ----------

eTrust AC :     2349

Last EntryId processed: 5167810102

Successfully detached from source [My_Audit_DSN]

Exiting Import...
```

Questa anteprima di importazione mostra che i l'intervallo di date produce un sottoinsieme più piccolo di eventi da importare. Ora è possibile eseguire l'importazione reale.

Ulteriori informazioni:

Nozioni fondamentali sulla riga di comando di LMSeosImport (a pagina 252)
Anteprima dei risultati dell'importazione (a pagina 256)

Importazione di eventi CA Access Control

Dopo avere eseguito l'importazione di eventi e un'anteprima dell'importazione, si è pronti per importare gli eventi CA Access Control dalla tabella SEOSDATA.

Per importare eventi CA Access Control

Utilizzare il comando dall'anteprima senza l'opzione -preview per ripristinare gli eventi CA Access Control dall'intervallo di date indicato:

```
LMSeosImport.exe –dsn [My_Audit_DSN] –user sa –password sa -target [My-CA-ELM-Server] –log "eTrust Access Control" -mintm 2008-11-01 -maxtm 2009-12-31
```

L'utilità visualizza i risultati come il seguente:

```
Import started on Fri Jan  2 15:41:23 2009


No transport specified, defaulting to SAPI...

Preparing ODBC connections...

Successfully attached to source [My_Audit_DSN]

No starting ENTRYID specified, using minimum ENTRYID of 1...

Import running, please wait...

.........

Import Completed (143762 records in 5 minutes 18 seconds).

---------- Imported Events (preview) By Log ----------

eTrust AC :     2241

Last EntryId processed: 5167810102

Successfully detached from source [My_Audit_DSN]

Exiting Import...
```

Ulteriori informazioni:

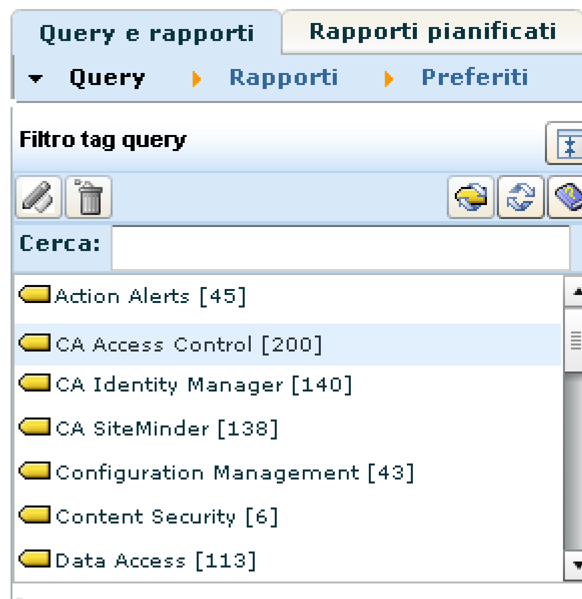
Nozioni fondamentali sulla riga di comando di LMSeosImport (a pagina 252)
Importazione di eventi da un database Windows Collector (a pagina 257)
Importazione di eventi da un database Solaris Collector (a pagina 257)

Visualizzazione di query e rapporti per la visualizzazione di eventi di CA Access Control

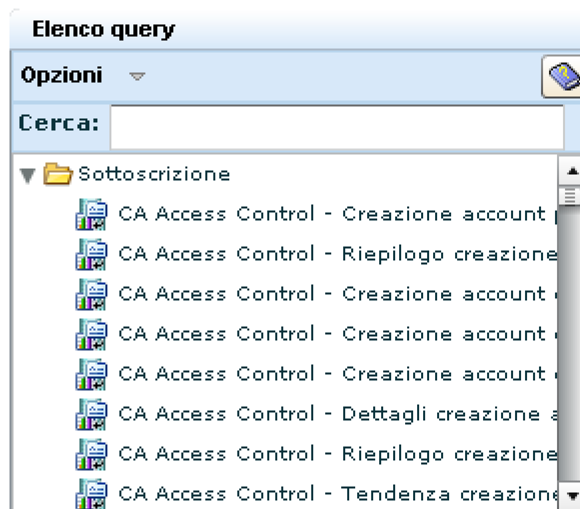
CA Enterprise Log Manager fornisce una serie di query e rapporti per l'analisi di eventi raccolti da CA Access Control. Utilizzare le procedure che seguono per accedere alle query e ai rapporti di CA Access Control.

Per accedere alle query di CA Access Control

1. Accedere al server CA Enterprise Log Manager come utente con diritti di visualizzazione di query e rapporti.
2. Accedere alla sottoscheda Query nella scheda Query e rapporti, se non è già visualizzata.



3. Fare clic sul tag della query CA Access Control per visualizzare le query disponibili nell'elenco a sinistra.

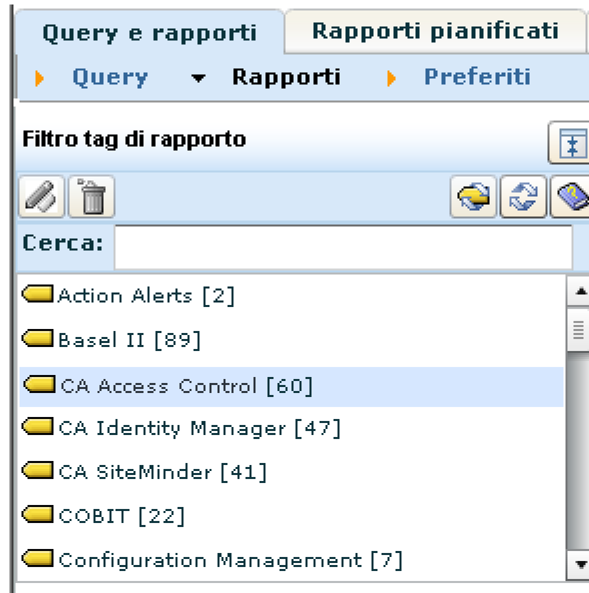


4. Selezionare una query per visualizzare i dati degli eventi.

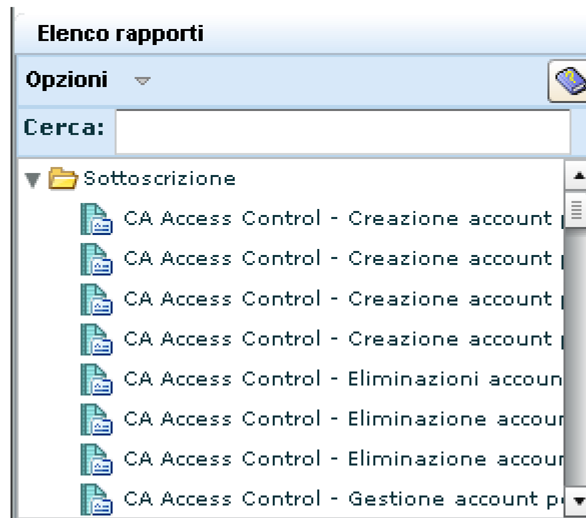
Per accedere ai rapporti di CA Access Control

1. Accedere al server CA Enterprise Log Manager come utente con diritti di visualizzazione di query e rapporti.

2. Accedere alla sottoscheda Rapporti nella scheda Query e rapporti, se non è già visualizzata.



3. Fare clic sul tag del rapporto CA Access Control per visualizzare i rapporti disponibili nell'elenco a sinistra.



4. Selezionare un rapporto per visualizzare i dati degli eventi.

Appendice C: Considerazioni su CA IT PAM

Questa sezione contiene i seguenti argomenti:

Scenario: utilizzo di CA EEM in CA Enterprise Log Manager per l'autenticazione CA IT PAM

Questa appendice illustra lo scenario in cui si desidera installare CA IT PAM su un server Windows e condividere CA EEM sul server CA Enterprise Log Manager per l'autenticazione. Queste procedure completano le procedure descritte nella guida *CA IT Process Automation Installation Guide*.

Importante: La condivisione di CA EEM *non è* supportata in modalità FIPS poiché CA IT PAM non è compatibile con la modalità FIPS. Se si esegue l'aggiornamento del server CA Enterprise Log Manager in modalità FIPS, l'integrazione con CA IT PAM non verrà eseguita.

Nota: se si desidera installare CA IT PAM su un server UNIX o utilizzare LDAP o CA EEM in locale per l'autenticazione, la documentazione in questa appendice non è adeguata. In questi casi, non si tratta di una condivisione di uno stesso server CA EEM. CA Enterprise Log Manager r12.1 SP1 può essere eseguito in modalità FIPS ed è in grado di comunicare con CA IT PAM; tuttavia, i canali di comunicazione non sono compatibili con la modalità FIPS.

Per ogni scenario di installazione, scaricare la *Guida all'installazione* di CA IT Process Automation Manager r2.1 SP03 dal supporto tecnico in linea. Inoltre, scaricare Adobe Acrobat Reader per poter aprire il documento in PDF.

Il processo che consente di utilizzare CA EEM su CA Enterprise Log Manager per l'autenticazione CA IT PAM comprende due passaggi manuali. È necessario copiare un file dal server Windows all'applicazione e un altro file dall'applicazione al server Windows. Queste operazioni vengono illustrate in questa appendice. Non vengono presentate nella documentazione di CA IT PAM.

Processo di implementazione di CA IT PAM

Il processo di implementazione dell'autenticazione di CA IT PAM tramite CA EEM sul server di gestione CA Enterprise Log Manager è indicato di seguito:

1. Preparare l'implementazione dell'autenticazione di CA IT PAM.
    a. Caricare il pacchetto di installazione di CA IT PAM sul server Windows su cui si desidera installare CA IT PAM.
    b. (Facoltativo) Modificare la password predefinita per il certificato itpamcert.p12.

2. Copiare il file ITPAM_eem.xml dall'host in cui si desidera installare CA IT PAM all'applicazione CA Enterprise Log Manager che include CA EEM.
3. Registrare ITPAM come istanza dell'applicazione sullo stesso CA EEM utilizzato da CA Enterprise Log Manager. L'esecuzione del comando safex genera il certificato itpamcert.p12 e l'istanza dell'applicazione ITPAM con due account utente, itpamadmin e itpamuser.

   Nota: per informazioni sull'utilizzo del comando safex, digitare /safex.
4. Copiare il file dal itpamcert.p12 dall'applicazione CA Enterprise Log Manager nell'host in cui si desidera installare il dominio di CA IT PAM.
5. Individuare l'applicazione ITPAM e reimpostare le password per itpamadmin e itpamuser.
6. Accedere al server Windows e installare i componenti di terze parti utilizzando le procedure descritte nella *Guida all'installazione di CA IT Process Automation Manager*.
7. Installare il dominio CA IT PAM utilizzando le istruzioni presentate in questa appendice e nelle istruzioni di installazione di CA IT PAM.
8. Avviare il servizio server CA ITPAM.
9. Avviare ed accedere alla console CA IT PAM.

Preparazione dell'implementazione dell'autenticazione di CA IT PAM su un CA EEM condiviso

In seguito al caricamento del pacchetto di installazione sul server Windows in cui si desidera installare il dominio CA IT PAM, è possibile impostare una password per il certificato itpamcert.cer.

Per preparare l'implementazione dell'autenticazione di CA IT PAM sul server di gestione di CA Enterprise Log Manager

1. Estrarre l'immagine ISO di CA IT PAM per l'host Windows Server 2003 in cui si desidera installare CA IT PAM.

   Nota: è possibile trovare l'immagine ISO di CA IT PAM sul CD 2 dell'origine dell'installazione.di CA IT PAM.

2. (Facoltativo) Modificare la password predefinita per il certificato IT PAM.

   a. Andare alla cartella <percorso di installazione>\eem.

   b. Aprire il file ITPAM_eem.xml

   c. Sostituire "itpamcertpass" nella seguente linea:

   ```
   <Register certfile="itpamcert.p12" password="itpamcertpass"/>
   ```

   d. Salvare il file.

Copiare un file XML nella Gestione di CA Enterprise Log Manager

Il comando safex genera oggetti di protezione CA IT PAM dal file ITPAM_eem.xml. È necessario copiare il file nell'applicazione CA Enterprise Log Manager in cui è possibile accedervi durante l'elaborazione di safex.

Per copiare il file ITPAM_eem.xml nell'applicazione CA Enterprise Log Manager

Copiare il file ITPAM_eem.xml disponibile sul disco di installazione di CA IT PAM nell'applicazione CA Enterprise Log Manager che include CA EEM. Se il file ISO è stato estratto sul server Windows, utilizzare Winscp per copiare ITPAM_eem.xml nella directory /tmp dell'applicazione.

- File di origine sul disco di installazione di CA IT PAM:

  ```
  ITPAM_eem.xml
  ```

- Percorso di destinazione sulla gestione CA Enterprise Log Manager:

  ```
  /opt/CA/SharedComponents/iTechnology
  ```

Registrazione di CA IT PAM con CA EEM condiviso

È possibile registrare CA IT PAM con CA EEM incorporato nel server di gestione di CA Enterprise Log Manager. La registrazione con CA EEM crea oggetti di protezione di CA IT PAM.

Gli oggetti di protezione di CA IT PAM aggiunti a CA EEM durante la registrazione sono i seguenti:

- Istanza dell'applicazione, ITPAM
- Criteri relativi all'accesso a CA IT PAM
- Gruppi e utenti, inclusi ITPAMAdmins, ITPAMUsers, itpamadmin, e itpamuser predefiniti
- Il certificato, itpamcert.p12

È possibile creare oggetti di protezione di CA IT PAM sul server di gestione CA Enterprise Log Manager. Prima di iniziare, è necessario ottenere la password caelmadmin se non si dispone già di essa.

Per registrare CA IT PAM con CA EEM sul server di gestione CA Enterprise Log Manager

1. Accedere all'applicazione CA Enterprise Log Manager attraverso ssh in qualità di utente caelmadmin.
2. Commutare gli utenti sull'account root.

   ```
   su -
   ```

3. Modificare le directory nel percorso di destinazione ed elencare il contenuto.

   ```
   cd /opt/CA/SharedComponents/iTechnology
   ls
   ```

4. Verificare che i seguenti file siano elencati:
   - ITPAM_eem.xml
   - safex

5. Eseguire il comando:

```
./safex -h <nome host ELM> -u EiamAdmin -p <password> -f ITPAM_eem.xml
```

   Il processo crea l'applicazione di CA IT PAM nel server di gestione di CA Enterprise Log Manager, aggiunge gli utenti predefiniti e genera il certificato necessario durante l'installazione di CA IT PAM. Il certificato è stato generato con la password specificata nel file ITPAM_eem.xml, o se non è stato modificato, itpamcertpass.

   Nota: per informazioni sull'utilizzo del comando safex, digitare /safex.

6. Elencare il contenuto della directory e verificare che il fileitpamcert.cer esista.

7. Rimuovere il file XML di configurazione di CA IT PAM. Si consiglia di eseguire questa operazione per motivi di protezione.

```
rm ITPAM_eem.xml
```

Copia del certificato sul server di CA IT PAM

Quando viene eseguito il comando safex da CA Enterprise Log Manager per la registrazione di CA IT PAM con CA EEM, il processo genera il certificato itpamcert.p12. È necessario copiare il certificato sul server Windows in cui si desidera installare il dominio di CA IT PAM. durante l'installazione del dominio di CA IT PAM, individuare il file del certificato.

Per copiare il certificato dall'applicazione CA Enterprise Log Manager sul server Windows di destinazione

Copiare il file dal itpamcert.p12 dall'applicazione CA Enterprise Log Manager che include CA EEM nell'host in cui si desidera installare CA IT PAM.

- File di origine sul server di gestione CA Enterprise Log Manager:

```
/opt/CA/SharedComponents/iTechnology/itpamcert.p12
```

- Percorso di destinazione sul server Windows di destinazione:

```
<percorso di installazione>
```

  Nota: è possibile copiare questo file nel percorso desiderato. È possibile selezionare il file dal percorso quando si installa il dominio di CA IT PAM.

Impostazione di password per gli account utente predefiniti di CA IT PAM

L'esecuzione del comando safex crea quanto segue:

- Gruppi di protezione IT PAM:
  - ITPAMAdmins
  - ITPAMUsers
- Utenti IT PAM
  - itpamadmin con una password predefinita
  - itpamuser con una password predefinita

È necessario reimpostare la password per i due utenti predefiniti di CA IT PAM.

Per reimpostare le password per itpamadmin e itpamuser nell'applicazione CA IT PAM in CA EEM

1. Individuare la URL del server in cui è installato CA EEM utilizzato da CA Enterprise Log Manager, ad esempio, il server di gestione CA Enterprise Log Manager:

   ```
   https://<server di gestione ELM>5250/spin/eiam
   ```

   Viene visualizzata la schermata di accesso di CA EEM. L'elenco a discesa dell'applicazione include <Global> CAELM e ITPAM.

2. Accedere all'applicazione IT PAM:

   a. Selezionare ITPAM come applicazione.

   b. Digitare EiamAdmin come nome utente.

   c. Specificare la password per l'account utente EiamAdmin.

   d. Fare clic su Accedi.

3. Selezionare la scheda Manage Identities (Gestione identità).

4. Nella finestra di dialogo Search Users (Ricerca utenti), immettere itpam come valore e fare clic su Vai.

   I seguenti utenti vengono visualizzati nell'elenco

   - itpamadmin
   - itpamuser

5. Reimpostare la password per itpamadmin:
   a. Selezionare itpamadmin dall'elenco e scorrere fino all'autenticazione nel riquadro destro.
   b. Selezionare Reset password (Reimposta password).
   c. Digitare la password dell'account nel campo Nuova password e Conferma password.
   d. Fare clic su Salva.
6. Reimpostare la password per itpamuser:
   a. Selezionare itpamuser dall'elenco e scorrere fino all'autenticazione nel riquadro destro.
   b. Selezionare Reset password (Reimposta password).
   c. Digitare la password dell'account nel campo Nuova password e Conferma password.
   d. Fare clic su Salva.
7. Fare clic su Disconnetti.

Installare i componenti di terze parti richiesti da CA IT PAM

Prima di installare i componenti di terze parti, occorre aver installato sul sistema JDK 1.6 o superiore. Eseguire Third_Party_Installer_windows.exe sul server Windows sul quale si intende installare CA IT PAM. Per ulteriori informazioni, consultare la *Guida all'installazione di CA IT Process Automation Manager*.

Installazione del dominio CA IT PAM

L'esecuzione della procedura guidata di CA IT PAM con le specifiche qui descritte fornisce un collegamento con il certificato in modo che CA IT PAM e CA EEM sul server di gestione CA Enterprise Log Manager risultino attendibili.

Avere a portata di mano le seguenti informazioni:

- Password per il file di certificato EEM, itpamcert.p12. È possibile che il file predefinito ITPAM_eem.xml sia stato modificato durante la fase Preparazione dell'implementazione dell'autenticazione di CA IT PAM su un CA EEM condiviso.
- Il nome host del server di gestione CA Enterprise Log Manager. Questo è il server in cui l'utente ha effettuato l'accesso durante la fase Registrazione di CA IT PAM con CA EEM condiviso.
- La password itpamadmin impostata durante la fase Impostazione di password per gli account utente predefiniti di CA IT PAM.
- La password del certificato utilizzata per controllare l'accesso alle chiavi utilizzate per crittografare le password. Questa è una nuova impostazione.

Per istruzioni sull'installazione del dominio di CA IT PAM, consultare la guida *CA IT Process Automation Manager Installation Guide*. Utilizzare la seguente procedura per specifiche sulla configurazione delle impostazioni di protezione di EEM.

Per installare il dominio CA IT PAM

1. Se l'installazione guidata di CA IT PAM non viene avviata in seguito all'installazione dei componenti di terze parti, eseguire il file CA_ITPAM_Domain_windows.exe.
2. Seguire le istruzioni fornite nella documentazione di CA IT PAM fino a Select Security Server Type (Selezionare il tipo di server di protezione).
3. Quando viene visualizzata la finestra di dialogo Select Security Server Type, selezionare EEM come server di protezione e fare clic su Avanti.

   Viene visualizzata la pagina delle impostazioni di protezione di EEM.

4. Completare le impostazioni di protezione di EEM come segue:
   a. Immettere il nome host del server di gestione CA Enterprise Log Manager nel campo Server EEM.
   b. Immettere ITPAM nel campo relativo all'applicazione EEM.
   c. Fare clic su Sfoglia e selezionare la cartella in cui posizionare itpamcert.p12.
   d. Selezionare itpamcert.p12.
   e. Completare il campo Password certificato EEM in uno dei seguenti modi:
      - Immettere la password che è stata sostituita nel file ITPAM_eem.xml durante la fase di preparazione.
      - Immettere itpamcertpass, la password predefinita.
5. Fare clic sulle impostazioni EEM.

   Viene visualizzato il messaggio "Performing a test...may take a few minutes" (Test in corso, l'operazione potrebbe richiedere qualche minuto).
6. Fare clic su OK.

   Viene visualizzata la finestra di dialogo di verifica delle impostazioni di EEM.
7. Immettere itpamadmin come nome utente. Immettere la password per l'account utente itpamadmin e fare clic su OK.
8. Fare clic su Avanti. Attenersi alle istruzioni documentate di CA IT PAM per completare il resto della procedura guidata.

Avviare il servizio server CA ITPAM

Avviare il servizio server CA ITPAM in modo da poter avviare il server CA IT PAM.

Avviare il servizio server CA ITPAM

1. Accedere al server Windows su cui è installato il dominio di CA IT PAM.
2. Dal menu Start, selezionare Programmi, Dominio ITPAM, Avvia servizio server.

   Nota: se non viene visualizzata l'opzione di menu, selezionare Strumenti di amministrazione, Servizi componente. Fare clic su Servizi, Server CA IT PAM e quindi su Avvia il servizio.

Avviare ed accedere alla console del server CA IT PAM.

È possibile avviare il server CA IT PAM da un browser su qualunque sistema sul quale siano installate e integrate le API di Java JRE 1.6 o di JDK 1.6.

Per avviare la console di gestione di CA IT PAM

1. Digitare l'URL seguente nella barra dell'indirizzo di un browser:

   ```
   http://<itpam_server_hostname>:8080/itpam/
   ```

   Viene visualizzata la schermata di accesso a CA IT Process Automation Manager.

2. Immettere itpamadmin nel campo Accesso utente.
3. Nel campo Password, immettere la password che è stata assegnata a questo account.
4. Fare clic su Accedi.

   L'CA EEM sul server CA Enterprise Log Manager esegue l'autenticazione delle credenziali di accesso e apre il CA IT Process Automation Manager.

Per informazioni dettagliate sull'integrazione e l'utilizzo di CA IT PAM con CA Enterprise Log Manager, consultare la sezione "Utilizzo dei processi di output/evento di CA IT PAM" nel capitolo Avvisi nella *Guida all'amministrazione* di *CA Enterprise Log Manager*.

Appendice D: Ripristino di emergenza

Questa sezione contiene i seguenti argomenti:

Pianificazione di un ripristino di emergenza

La pianificazione di un ripristino di emergenza costituisce una parte necessaria di ogni buon piano di amministrazione di una rete. La pianificazione del ripristino di emergenza CA Enterprise Log Manager è relativamente semplice e diretta. È essenziale per un ripristino di emergenza efficace per CA Enterprise Log Manager effettuare backup regolari.

È necessario eseguire backup delle seguenti informazioni:

- Istanza dell'applicazione CA Enterprise Log Manager sul server di gestione
- Cartella /opt/CA/LogManager/data di ogni server CA Enterprise Log Manager
- File dei certificati nella cartella /opt/CA/SharedComponents/iTechnology di ogni server CA Enterprise Log Manager

Se è essenziale mantenere livelli di velocità elevati per l'implementazione, si può scegliere di avere un server di riserva con le stesse caratteristiche hardware di quello su cui si installano gli altri server CA Enterprise Log Manager. Se un server CA Enterprise Log Manager è disabilitato, è possibile installarne un altro utilizzando lo stesso identico nome. Quando viene avviato il nuovo server, esso riceve i file di configurazione necessari dal server di gestione. Se questo livello di prestazioni non è essenziale per l'implementazione, è possibile installare un server CA Enterprise Log Manager su qualsiasi server vuoto in grado di ospitare il sistema operativo di base e di soddisfare i requisiti minimi di memoria e disco rigido.

Ulteriori informazioni sui requisiti hardware e software sono disponibili nelle *Note di rilascio CA Enterprise Log Manager*.

Anche il server interno CA EEM, installato nel server di gestione, dispone dei suoi processi di configurazione failover per garantire la continuità delle operazioni, esaminate in dettaglio nella *Guida introduttiva CA EEM*.

Informazioni sul backup del server CA EEM

La configurazione di ogni server, agente e connettore CA Enterprise Log Manager, oltre che di query, rapporti, avvisi e altro ancora, viene conservata separatamente nel repository CA EEM del server CA Enterprise Log Manager di gestione. L'elemento fondamentale del ripristino corretto di un server è l'esecuzione di backup regolari delle informazioni conservate nell'istanza dell'applicazione CA Enterprise Log Manager.

Un'*istanza dell'applicazione* è uno spazio comune all'interno del repository CA EEM che conserva le seguenti informazioni:

- Utenti, gruppi e criteri di accesso
- Agente, integrazione, listener, connettore e configurazioni salvate
- Query personalizzate, rapporti e regole di soppressione e di riepilogo
- Relazioni di federazione
- Informazioni di gestione del codice binario
- Chiavi di crittografia

È possibile eseguire la procedura di backup CA EEM dall'interno dell'interfaccia del browser web CA EEM. Solitamente, tutti i server CA Enterprise Log Manager in un'azienda utilizzano la stessa istanza dell'applicazione. Il valore predefinito dell'istanza dell'applicazione CA Enterprise Log Manager è CAELM. È possibile installare server CA Enterprise Log Manager con istanze delle applicazioni diverse, ma è possibile federare solo i server che condividono la stessa istanza dell'applicazione. I server configurati per utilizzare lo stesso server CA EEM, ma con istanze delle applicazioni diverse, condividono solo l'archivio utente, i criteri delle password e i gruppi globali.

La *Guida introduttiva di CA EEM* contiene ulteriori informazioni sulle operazioni di backup e di ripristino.

Backup dell'istanza dell'applicazione CA EEM

È possibile eseguire il backup dell'istanza dell'applicazione CA Enterprise Log Manager dal server CA EEM interno sul server di gestione.

Per eseguire il backup dell'istanza dell'applicazione

1. Accedere al server CA EEM con il seguente URL:

   `https://<nomeserver>:5250/spin/eiam`

2. Espandere l'elenco Applicazioni nella pagina di accesso e selezionare il nome dell'istanza dell'applicazione utilizzata durante l'installazione dei server CA Enterprise Log Manager.

   Il nome istanza dell'applicazione predefinito per CA Enterprise Log Manager è CAELM.

3. Accedere come utente EiamAdmin o utente con ruolo di amministratore CA EEM.
4. Accedere alla scheda Configura e selezionare la sottoscheda Server EEM.
5. Selezionare la voce Esporta applicazione nel riquadro di navigazione a sinistra.
6. Selezionare tutte le opzioni eccetto la casella di controllo Ignora dimensioni massime di ricerca.

   Nota: se si sta utilizzando una directory esterna, non selezionare le opzioni Utenti globali, Gruppi globali e cartelle globali.

7. Fare clic su Esporta per creare un file di esportazione XML per l'istanza dell'applicazione.

   La finestra di dialogo Download file visualizza il nome del file, *<NomeIstanzaAppl>*.xml.gz, ad esempio CAELM.xml.gz e il pulsante Salva.

8. Fare clic su Salva e selezionare la posizione di backup su un server remoto mappato. Oppure salvare il file localmente e copiarlo o spostarlo nella posizione di backup su un altro server.

Ripristino di un server CA EEM per l'utilizzo con CA Enterprise Log Manager

È possibile ripristinare un'istanza dell'applicazione CA Enterprise Log Manager in un server di gestione. Il ripristino della funzionalità CA EEM del server di gestione implica l'esecuzione dell'utilità safex che importa l'istanza dell'applicazione di cui è stato eseguito il backup.

Per ripristinare la funzionalità CA EEM del server di gestione da un backup

1. Installare il dispositivo software CA Enterprise Log Manager su un server con hardware nuovo.
2. Accedere a un prompt dei comandi e navigare fino alla directory /opt/CA/LogManager/EEM.
3. Copiare il file del backup <*Nomeistanzaapp*>.xml.gz in questa directory dal server di backup esterno.
4. Eseguire il seguente comando per recuperare il file di esportazione XML:

   ```
   gunzip <Nomeistanzaapp>.xml.gz
   ```

5. Eseguire il seguente comando per ripristinare il file di esportazione sul nuovo server di gestione

   ```
   ./safex –h eemserverhostname –u EiamAdmin –p password –f AppinstanceName.xml
   ```

   Se si sta utilizzando la modalità FIPS, verificare che l'opzione -fips sia inclusa.
6. Navigare fino alla directory /opt/CA/ELMAgent/bin.
7. Sostituire il file predefinito AgentCert.cer con il file del backup CAELM_AgentCert.cer per garantire un avvio corretto dell'agente.

Backup di un server CA Enterprise Log Manager

È possibile eseguire il backup di un intero server CA Enterprise Log Manager dalla cartella /opt/CA/LogManager/data. La cartella dei dati è un collegamento simbolico alla cartella dati sotto la directory root (/data).

Per eseguire il backup di un server CA Enterprise Log Manager

1. Accedere al server CA Enterprise Log Manager come utente caelmadmin.
2. Accedere all'account root utilizzando l'utilità su.
3. Navigare fino alla directory /opt/CA/LogManager.
4. Eseguire il seguente comando TAR per creare una copia di backup dei file del server CA Enterprise Log Manager:

   ```
   tar –hzcvf backupData.tgz /data
   ```

   Questo comando crea il file di output compresso backupData.tgz utilizzando i file della directory /data.

5. Navigare fino alla directory /opt/CA/SharedComponents/iTechnology.
6. Eseguire il seguente comando TAR per creare una copia di backup dei certificati digitali (tutti i file con estensione file .cer):

```
tar –zcvf backupCerts.tgz *.cer
```

Questo comando crea il file di output compresso backupCerts.tgz.

```
tar –hzcvf backupCerts.tgz /data
```

Ripristino di un server CA Enterprise Log Manager da file di backup

È possibile ripristinare un server CA Enterprise Log Manager da file di backup dopo avere installato il dispositivo software CA Enterprise Log Manager sul nuovo server.

Per ripristinare un server CA Enterprise Log Manager da backup

1. Terminare il processo iGateway sul nuovo server.

   Per effettuare quest'operazione, navigare fino alla cartella /opt/CA/SharedComponents/iTechnology ed eseguire il seguente comando:

   ```
   ./S99igateway stop
   ```

2. Copiare i file backupData.tgz e backupCerts.tgz nella directory /opt/CA/LogManager sul nuovo server.
3. Espandere il contenuto del file backupData.tgz con il seguente comando:

   ```
   tar –xzvf  backupData.tgz
   ```

   Questo comando sovrascrive il contenuto della cartella dei dati con il contenuto del file di backup.

4. Navigare fino alla directory /opt/CA/SharedComponents/iTechnology.
5. Espandere il contenuto del file backupCerts.tgz con il seguente comando:

   ```
   tar –xzvf  backupCerts.tgz
   ```

   Questo comando sovrascrive i file dei certificati (.p12) nella cartella corrente con i file dei certificati dal file di backup.

6. Avviare il servizio igateway.

   Per effettuare questa operazione, eseguire il seguente comando:

   ```
   ./S99igateway start
   ```

Sostituzione di un server CA Enterprise Log Manager

Utilizzare questa procedura per sostituire una raccolta di server CA Enterprise Log Manager in seguito a un'emergenza o a un guasto serio. Questa procedura permette di eseguire il ripristino da una situazione di emergenza creando un nuovo server CA Enterprise Log Manager per riprendere la raccolta di eventi al posto del server guasto.

Nota: questo procedura non ripristina i dati degli eventi che risiedono nell'archivio registro eventi del server guasto. Utilizzare tecniche di ripristino regolare dei dati per ripristinare dati degli eventi dall'archivio registro eventi del server guasto.

Per eseguire il ripristino da un server CA Enterprise Log Manager disabilitato

1. Installare il dispositivo software CA Enterprise Log Manager su un server diverso utilizzando lo stesso nome host assegnato al server guasto.

   Quando l'installazione richiede il nome dell'istanza dell'applicazione CA EEM, assicurarsi di utilizzare lo stesso nome di istanza dell'applicazione utilizzato per il vecchio server. Questa registrazione corretta permette al server CA EEM di sincronizzare la configurazione.

2. Avviare il nuovo server CA Enterprise Log Manager e accedere come utente amministratore predefinito EiamAdmin.

   Quando il nuovo server CA Enterprise Log Manager si avvia, si connette automaticamente al server CA EEM, che a sua volta scaricherà i file di configurazione. Dopo avere ricevuto i file di configurazione, il nuovo server CA Enterprise Log Manager riprende la raccolta dei log.

Appendice E: CA Enterprise Log Manager e virtualizzazione

Questa sezione contiene i seguenti argomenti:

Ipotesi di distribuzione

Utilizzando CA Enterprise Log Manager in un ambiente virtuale o in un ambiente misto che includa sia server a livello di dispositivo che virtuali, si parte dai seguenti presupposti:

- In un ambiente interamente virtuale, installare almeno un server CA Enterprise Log Manager come server di gestione. Tale server di gestione gestisce le configurazioni, il contenuto della sottoscrizione, il contenuto definito dall'utente e le comunicazioni con gli agenti. Il server di gestione non riceve i registri eventi né gestisce le query e i rapporti.
- In un ambiente misto, installare il server CA Enterprise Log Manager di gestione su hardware certificato.
- Ogni host di macchine virtuali deve avere quattro processori dedicati, il numero massimo consentito da VMware ESX Server 3.5.

Considerazioni

Un server CA Enterprise Log Manager dedicato raggiunge prestazioni ottimali con otto o più processori. VMware ESX Server consente di avere fino a quattro processori su un'unica macchina virtuale. Per ottenere prestazioni simili a un server dedicato a otto processori, installare CA Enterprise Log Manager su due o più macchine virtuali e federarle per i rapporti consolidati.

Due server CA Enterprise Log Manager in esecuzione come guest in VMware ESX Server v3.5 raggiungono una capacità paragonabile a quella di un unico server CA Enterprise Log Manager dedicato. Utilizzare la seguente tabella per agevolare la pianificazione della rete virtuale:

Ruolo server CA Enterprise Log Manager	**Numero di processori (minimo)**	**Velocità della CPU in GHz (per CPU)**	**Memoria totale in GB (requisito minimo)**
Gestione	8	3	8
Rapporti	8	3	8
Raccolta	4	3	8

Nota: il numero massimo di eventi per secondo è 1K. In configurazioni di distribuzione medie è 1K mentre in configurazioni di distribuzione estese è 5 KB.

Creazione di server CA Enterprise Log Manager mediante computer virtuali

È possibile creare server CA Enterprise Log Manager virtuali per il proprio ambiente di raccolta log eventi, utilizzando i seguenti scenari:

- Aggiunta di server virtuali a un ambiente CA Enterprise Log Manager esistente: creazione di un ambiente misto
- Creazione di un ambiente di raccolta log virtuale
- Duplicazione e distribuzione di server CA Enterprise Log Manager virtuali per una rapida scalabilità
- Creazione di server CA Enterprise Log Manager mediante applicazioni virtuali

Ulteriori informazioni

Aggiunta di server virtuali all'ambiente (a pagina 325)
Creazione di un ambiente completamente virtuale (a pagina 348)
Distribuzione rapida di server virtuali (a pagina 373)

Aggiunta di server virtuali all'ambiente

Se si dispone già di un'implementazione di CA Enterprise Log Manager, è possibile aggiungere server di raccolta CA Enterprise Log Manager per gestire un volume di eventi in aumento nella rete. Questo scenario dà per scontato che sia già stato installato un server di gestione CA Enterprise Log Manager e uno o più server CA Enterprise Log Manager per la raccolta e i rapporti.

Nota: per ottenere le migliori prestazioni, installare CA Enterprise Log Manager su server virtuali per gestire solo attività di raccolta e rapporti.

La procedura per l'aggiunta di server di raccolta virtuali all'ambiente include le seguenti procedure:

1. Creazione di una nuova macchina virtuale.
2. Aggiunta di unità disco virtuali.
3. Installazione di CA Enterprise Log Manager sulla macchina virtuale.
4. Configurazione del server CA Enterprise Log Manager come descritto nella sezione sull'installazione.

Dopo avere installato il server di raccolta virtuale, è possibile aggiungerlo alla federazione per le query e i rapporti.

Creazione di una nuova macchina virtuale

Utilizzare questa procedura per creare una nuova macchina virtuale utilizzando VMware Infrastructure Client. Utilizzare quattro processori affinché ogni server virtuale CA Enterprise Log Manager possa raggiungere prestazioni accettabili.

Per creare una macchina virtuale

1. Accedere a VMware Infrastructure Client.
2. Fare clic con il pulsante destro sull'host ESX nel riquadro a sinistra e selezionare Nuova macchina virtuale per richiamare la procedura guidata della nuova macchina virtuale. Questa azione visualizza una finestra di dialogo per la configurazione.
3. Selezionare una configurazione personalizzata e fare clic su Avanti. Verrà visualizzata una finestra di dialogo del nome e della posizione.

4. Immettere un nome per il server CA Enterprise Log Manager che verrà installato su questa macchina virtuale e fare clic su Avanti.
5. Specificare le impostazioni di archiviazione per la macchina virtuale e fare clic su Avanti.

   Verificare che le impostazioni di archiviazione siamo abbastanza grandi per il server CA Enterprise Log Manager. Si consiglia un minimo di 500 GB.

   Nota: si configureranno unito disco virtuale aggiuntive per l'archiviazione dei registri eventi raccolti in un'altra procedura.
6. Selezionare Red Hat Enterprise Linux 5 (32 bit) come sistema operativo guest e fare clic su Avanti.
7. Selezionare 4 come numero di processori virtuali dall'elenco a discesa Numero di processori virtuali.

   Il server host fisico deve essere in grado di dedicare quattro CPU fisiche *esclusivamente* a questa istanza di CA Enterprise Log Manager. Fare clic su Avanti.
8. Configurare le dimensioni della memoria della macchina virtuale e fare clic su Avanti. Le dimensioni di memoria *minime* accettabili per CA Enterprise Log Manager sono 8 GB o 8192 MB.
9. La configurazione della connessione dell'interfaccia di rete (NIC).CA Enterprise Log Manager richiede almeno una connessione di rete. Selezionare NIC x dall'elenco delle NIC disponibili e impostare il valore dell'Adapter in Flessibile.

   Nota: non è necessario configurare un NIC separato per ogni server CA Enterprise Log Manager ospitato su questo server fisico. Tuttavia, è necessario allocare e assegnare un indirizzo IP statico per ognuno.
10. Selezionare l'opzione Connetti all'accensione e fare clic su Avanti. Verrà visualizzata la finestra di dialogo Tipi di adapter I/O.
11. Selezionare LSI Logic per l'Adapter I/O e fare clic su Avanti. Verrà visualizzata la finestra di dialogo Selezione disco.
12. Selezionare l'opzione Crea nuovo disco virtuale e fare clic su Avanti. Verrà visualizzata una finestra di dialogo della capacità e della posizione del disco.

13. Specificare la capacità e la posizione del disco e fare clic su Avanti. Verrà visualizzata la finestra di dialogo opzioni avanzate.

    È possibile archiviare il disco con la macchina virtuale o specificare un'altra posizione. Si consiglia un minimo di 500 GB.

14. Accettare i valori predefiniti per le Opzioni avanzate e fare clic su Avanti.
15. Confermare le impostazioni e fare clic su Fine per creare la nuova macchina virtuale.

Aggiunta di unità disco virtuali

Utilizzare questa procedura per aggiungere unità disco virtuali per l'archiviazione dei registri eventi. Utilizzare le stesse impostazioni a prescindere dal ruolo che un server CA Enterprise Log Manager specifico svolge all'interno della rete.

Per modificare le impostazioni

1. fare clic con il pulsante destro sulla macchina virtuale in VMware Infrastructure Client e selezionare Modifica impostazioni.

   Verrà visualizzata la finestra di dialogo Proprietà macchina virtuale.

2. Evidenziare le proprietà dell'Unità CD/DVD 1.
3. Fare clic sul pulsante di opzione Periferica host e selezionare l'unità DVD-ROM dall'elenco a discesa.
4. Selezionare l'opzione Stato periferica, Connetti all'accensione.
5. Fare clic su Aggiungi per avviare l'Aggiunta hardware guidato e aggiungere un secondo disco rigido.
6. Evidenziare il disco rigido nell'elenco delle periferiche e fare clic su Avanti. Verrà visualizzata la finestra di dialogo Selezionare un disco.
7. Selezionare l'opzione Crea nuovo disco virtuale e fare clic su Avanti.

8. Specificare le dimensioni del nuovo disco e selezionare l'opzione Specificare un datastore per impostarne la posizione.

   CA Enterprise Log Manager rileva questa periferica aggiuntiva durante l'installazione e l'assegna all'archiviazione dei dati. Si consiglia di massimizzare la quantità di archiviazione da rendere disponibile per CA Enterprise Log Manager.

   Nota: l'impostazione Dimensione blocco in VMware ESX Server è 1 MB; ciò limita lo spazio massimo su disco che è possibile creare a 256 GB. Se è necessario più spazio, fino a 512 GB, aumentare l'impostazione Dimensione blocco a 2 MB utilizzando questo comando:

   ```
   Vmkfstools --createfs vmfs3 --blocksize 2M vmhba0:0:0:3
   ```

   Per rendere effettive le nuove impostazioni è necessario riavviare ESX Server. Ulteriori informazioni su questo e altri comandi sono disponibili nella documentazione di VMware ESX Server.

   fare clic su Avanti per visualizzare la finestra di dialogo Specificare opzioni avanzate.

9. Accettare i valori predefiniti per le Opzioni avanzate e fare clic su Avanti. Comparirà la finestra di dialogo Pronto per il completamento.

10. Fare clic su Fine per archiviare le modifiche a questa macchina virtuale. Questa azione restituisce la finestra di dialogo di VMware Infrastructure Client.

Installare CA Enterprise Log Manager sulla macchina virtuale

Utilizzare questa procedura per installare CA Enterprise Log Manager su una macchina virtuale creata in precedenza.

È possibile configurare un server CA Enterprise Log Manager virtuale o dedicato dopo l'installazione affinché svolga uno di diversi ruoli funzionali come gestione, raccolta o rapporti. Se si installa un server di gestione CA Enterprise Log Manager, non utilizzarlo per ricevere i registri eventi o per eseguire query e rapporti. Installare server virtuali CA Enterprise Log Manager separati che operino come server di rapporto e di raccolta per ottenere le prestazioni migliori.

Rivedere le istruzioni dell'installazione normale prima di installare CA Enterprise Log Manager in un ambiente virtuale. Il foglio di calcolo dell'installazione aiuta a raccogliere le informazioni necessarie.

Per installare CA Enterprise Log Manager in una macchina virtuale

1. Caricare il disco di installazione del SO CA Enterprise Log Manager nell'unità DVD-ROM fisica o localizzare la directory in cui è stata copiata l'immagine di installazione.
2. Evidenziare la macchina virtuale nell'elenco dell'inventario delle macchine virtuali, fare clic con il pulsante destro su di essa e selezionare Accendi.
3. Procedere con l'installazione normale di CA Enterprise Log Manager.
4. Configurare il server CA Enterprise Log Manager installato per il ruolo funzionale richiesto, utilizzando le informazioni nella sezione sull'installazione di un server CA Enterprise Log Manager.

Ulteriori informazioni

Installazione di CA Enterprise Log Manager (a pagina 85)

Creazione di un ambiente completamente virtuale

Se non è già stato implementato un ambiente CA Enterprise Log Manager, è possibile creare un ambiente di raccolta dei registri completamente virtuale. Questo scenario dà per scontato che sia disponibile un numero sufficiente di server, ognuno con un gruppo i almeno quattro processori, per installare ognuno dei server CA Enterprise Log Manager pianificati.

Installare un server CA Enterprise Log Manager per il funzionamento come server di gestione. Durante la configurazione, non inviare registri di eventi a questo server o utilizzare questo server per generare rapporti. La configurazione dell'ambiente in questo modo mantiene la velocità della raccolta di registri eventi richiesta per una produzione di livello aziendale.

Solitamente, si installano due server CA Enterprise Log Manager a quattro processori al posto di ogni server di classe dispositivo che solitamente si installerebbe quando si usa hardware certificato (i server di classe dispositivo dispongono di minimo otto processori).

Il processo di creazione di un ambiente virtuale include le seguenti procedure.

1. Creazione di una nuova macchina virtuale per ognuno dei server CA Enterprise Log Manager da installare.
2. Aggiunta di unità disco virtuali.
3. Installazione di un server CA Enterprise Log Manager virtuale per la funzioni di gestione in uno degli host della macchina virtuale.
4. Installazione di due o più server CA Enterprise Log Manager per la raccolta e i rapporti.
5. Configurazione dei server CA Enterprise Log Manager come descritto nella sezione sull'installazione di un server CA Enterprise Log Manager.

Creazione di una nuova macchina virtuale

Utilizzare questa procedura per creare una nuova macchina virtuale utilizzando VMware Infrastructure Client. Utilizzare quattro processori affinché ogni server virtuale CA Enterprise Log Manager possa raggiungere prestazioni accettabili.

Per creare una macchina virtuale

1. Accedere a VMware Infrastructure Client.
2. Fare clic con il pulsante destro sull'host ESX nel riquadro a sinistra e selezionare Nuova macchina virtuale per richiamare la procedura guidata della nuova macchina virtuale. Questa azione visualizza una finestra di dialogo per la configurazione.
3. Selezionare una configurazione personalizzata e fare clic su Avanti. Verrà visualizzata una finestra di dialogo del nome e della posizione.
4. Immettere un nome per il server CA Enterprise Log Manager che verrà installato su questa macchina virtuale e fare clic su Avanti.
5. Specificare le impostazioni di archiviazione per la macchina virtuale e fare clic su Avanti.

   Verificare che le impostazioni di archiviazione siamo abbastanza grandi per il server CA Enterprise Log Manager. Si consiglia un minimo di 500 GB.

   Nota: si configureranno unito disco virtuale aggiuntive per l'archiviazione dei registri eventi raccolti in un'altra procedura.
6. Selezionare Red Hat Enterprise Linux 5 (32 bit) come sistema operativo guest e fare clic su Avanti.

7. Selezionare 4 come numero di processori virtuali dall'elenco a discesa Numero di processori virtuali.

   Il server host fisico deve essere in grado di dedicare quattro CPU fisiche *esclusivamente* a questa istanza di CA Enterprise Log Manager. Fare clic su Avanti.

8. Configurare le dimensioni della memoria della macchina virtuale e fare clic su Avanti. Le dimensioni di memoria *minime* accettabili per CA Enterprise Log Manager sono 8 GB o 8192 MB.

9. La configurazione della connessione dell'interfaccia di rete (NIC).CA Enterprise Log Manager richiede almeno una connessione di rete. Selezionare NIC x dall'elenco delle NIC disponibili e impostare il valore dell'Adapter in Flessibile.

   Nota: non è necessario configurare un NIC separato per ogni server CA Enterprise Log Manager ospitato su questo server fisico. Tuttavia, è necessario allocare e assegnare un indirizzo IP statico per ognuno.

10. Selezionare l'opzione Connetti all'accensione e fare clic su Avanti. Verrà visualizzata la finestra di dialogo Tipi di adapter I/O.

11. Selezionare LSI Logic per l'Adapter I/O e fare clic su Avanti. Verrà visualizzata la finestra di dialogo Selezione disco.

12. Selezionare l'opzione Crea nuovo disco virtuale e fare clic su Avanti. Verrà visualizzata una finestra di dialogo della capacità e della posizione del disco.

13. Specificare la capacità e la posizione del disco e fare clic su Avanti. Verrà visualizzata la finestra di dialogo opzioni avanzate.

    È possibile archiviare il disco con la macchina virtuale o specificare un'altra posizione. Si consiglia un minimo di 500 GB.

14. Accettare i valori predefiniti per le Opzioni avanzate e fare clic su Avanti.

15. Confermare le impostazioni e fare clic su Fine per creare la nuova macchina virtuale.

Aggiunta di unità disco virtuali

Utilizzare questa procedura per aggiungere unità disco virtuali per l'archiviazione dei registri eventi. Utilizzare le stesse impostazioni a prescindere dal ruolo che un server CA Enterprise Log Manager specifico svolge all'interno della rete.

Per modificare le impostazioni

1. fare clic con il pulsante destro sulla macchina virtuale in VMware Infrastructure Client e selezionare Modifica impostazioni.

   Verrà visualizzata la finestra di dialogo Proprietà macchina virtuale.

2. Evidenziare le proprietà dell'Unità CD/DVD 1.
3. Fare clic sul pulsante di opzione Periferica host e selezionare l'unità DVD-ROM dall'elenco a discesa.
4. Selezionare l'opzione Stato periferica, Connetti all'accensione.
5. Fare clic su Aggiungi per avviare l'Aggiunta hardware guidato e aggiungere un secondo disco rigido.
6. Evidenziare il disco rigido nell'elenco delle periferiche e fare clic su Avanti. Verrà visualizzata la finestra di dialogo Selezionare un disco.
7. Selezionare l'opzione Crea nuovo disco virtuale e fare clic su Avanti.
8. Specificare le dimensioni del nuovo disco e selezionare l'opzione Specificare un datastore per impostarne la posizione.

   CA Enterprise Log Manager rileva questa periferica aggiuntiva durante l'installazione e l'assegna all'archiviazione dei dati. Si consiglia di massimizzare la quantità di archiviazione da rendere disponibile per CA Enterprise Log Manager.

   Nota: l'impostazione Dimensione blocco in VMware ESX Server è 1 MB; ciò limita lo spazio massimo su disco che è possibile creare a 256 GB. Se è necessario più spazio, fino a 512 GB, aumentare l'impostazione Dimensione blocco a 2 MB utilizzando questo comando:

   ```
   Vmkfstools --createfs vmfs3 --blocksize 2M vmhba0:0:0:3
   ```

   Per rendere effettive le nuove impostazioni è necessario riavviare ESX Server. Ulteriori informazioni su questo e altri comandi sono disponibili nella documentazione di VMware ESX Server.

   fare clic su Avanti per visualizzare la finestra di dialogo Specificare opzioni avanzate.

9. Accettare i valori predefiniti per le Opzioni avanzate e fare clic su Avanti. Comparirà la finestra di dialogo Pronto per il completamento.
10. Fare clic su Fine per archiviare le modifiche a questa macchina virtuale. Questa azione restituisce la finestra di dialogo di VMware Infrastructure Client.

Installare CA Enterprise Log Manager sulla macchina virtuale

Utilizzare questa procedura per installare CA Enterprise Log Manager su una macchina virtuale creata in precedenza.

È possibile configurare un server CA Enterprise Log Manager virtuale o dedicato dopo l'installazione affinché svolga uno di diversi ruoli funzionali come gestione, raccolta o rapporti. Se si installa un server di gestione CA Enterprise Log Manager, non utilizzarlo per ricevere i registri eventi o per eseguire query e rapporti. Installare server virtuali CA Enterprise Log Manager separati che operino come server di rapporto e di raccolta per ottenere le prestazioni migliori.

Rivedere le istruzioni dell'installazione normale prima di installare CA Enterprise Log Manager in un ambiente virtuale. Il foglio di calcolo dell'installazione aiuta a raccogliere le informazioni necessarie.

Per installare CA Enterprise Log Manager in una macchina virtuale

1. Caricare il disco di installazione del SO CA Enterprise Log Manager nell'unità DVD-ROM fisica o localizzare la directory in cui è stata copiata l'immagine di installazione.
2. Evidenziare la macchina virtuale nell'elenco dell'inventario delle macchine virtuali, fare clic con il pulsante destro su di essa e selezionare Accendi.
3. Procedere con l'installazione normale di CA Enterprise Log Manager.
4. Configurare il server CA Enterprise Log Manager installato per il ruolo funzionale richiesto, utilizzando le informazioni nella sezione sull'installazione di un server CA Enterprise Log Manager.

Ulteriori informazioni

Installazione di CA Enterprise Log Manager (a pagina 85)

Distribuzione rapida di server virtuali di CA Enterprise Log Manager

È possibile clonare un server CA Enterprise Log Manager virtuale per creare un'immagine distribuibile per la rapida scalabilità del proprio ambiente di raccolta registri.

Nota: per ottenere le prestazioni migliori, si consiglia di installare CA Enterprise Log Manager su server virtuali per gestire solamente le attività di raccolta. Non clonare una macchina virtuale contenente un server CA Enterprise Log Manager di gestione.

Prima di avviare questo scenario, verificare la presenza di un ambiente o installare un server CA Enterprise Log Manager per l'esecuzione delle funzioni di gestione su un server dedicato o virtuale. È inoltre necessario disporre della versione corretta del software VMware per supportare la funzione di clonazione.

Il processo seguito per la creazione e la clonazione di un server CA Enterprise Log Manager virtuale per la raccolta comprende le seguenti procedure:

1. Creazione di una nuova macchina virtuale.
2. Aggiunta di unità disco virtuali.
3. Installazione di un server CA Enterprise Log Manager sulla macchina virtuale.
4. Clonare la macchina virtuale contenente il nuovo server CA Enterprise Log Manager, secondo le istruzioni fornite dal fornitore.

   Nota: creare solamente un'immagine clonata intera. Non utilizzare clonazioni collegate con CA Enterprise Log Manager.
5. Importare la macchina clonata virtuale su un server fisico di destinazione.
6. Aggiornare la macchina virtuale clonata prima di collegarla alla rete.
7. Configurare il server CA Enterprise Log Manager come descritto nella *Guida all'implementazione*.

Creazione di una nuova macchina virtuale

Utilizzare questa procedura per creare una nuova macchina virtuale utilizzando VMware Infrastructure Client. Utilizzare quattro processori affinché ogni server virtuale CA Enterprise Log Manager possa raggiungere prestazioni accettabili.

Per creare una macchina virtuale

1. Accedere a VMware Infrastructure Client.
2. Fare clic con il pulsante destro sull'host ESX nel riquadro a sinistra e selezionare Nuova macchina virtuale per richiamare la procedura guidata della nuova macchina virtuale. Questa azione visualizza una finestra di dialogo per la configurazione.
3. Selezionare una configurazione personalizzata e fare clic su Avanti. Verrà visualizzata una finestra di dialogo del nome e della posizione.

4. Immettere un nome per il server CA Enterprise Log Manager che verrà installato su questa macchina virtuale e fare clic su Avanti.
5. Specificare le impostazioni di archiviazione per la macchina virtuale e fare clic su Avanti.

   Verificare che le impostazioni di archiviazione siamo abbastanza grandi per il server CA Enterprise Log Manager. Si consiglia un minimo di 500 GB.

   Nota: si configureranno unito disco virtuale aggiuntive per l'archiviazione dei registri eventi raccolti in un'altra procedura.
6. Selezionare Red Hat Enterprise Linux 5 (32 bit) come sistema operativo guest e fare clic su Avanti.
7. Selezionare 4 come numero di processori virtuali dall'elenco a discesa Numero di processori virtuali.

   Il server host fisico deve essere in grado di dedicare quattro CPU fisiche *esclusivamente* a questa istanza di CA Enterprise Log Manager. Fare clic su Avanti.
8. Configurare le dimensioni della memoria della macchina virtuale e fare clic su Avanti. Le dimensioni di memoria *minime* accettabili per CA Enterprise Log Manager sono 8 GB o 8192 MB.
9. La configurazione della connessione dell'interfaccia di rete (NIC).CA Enterprise Log Manager richiede almeno una connessione di rete. Selezionare NIC x dall'elenco delle NIC disponibili e impostare il valore dell'Adapter in Flessibile.

   Nota: non è necessario configurare un NIC separato per ogni server CA Enterprise Log Manager ospitato su questo server fisico. Tuttavia, è necessario allocare e assegnare un indirizzo IP statico per ognuno.
10. Selezionare l'opzione Connetti all'accensione e fare clic su Avanti. Verrà visualizzata la finestra di dialogo Tipi di adapter I/O.
11. Selezionare LSI Logic per l'Adapter I/O e fare clic su Avanti. Verrà visualizzata la finestra di dialogo Selezione disco.
12. Selezionare l'opzione Crea nuovo disco virtuale e fare clic su Avanti. Verrà visualizzata una finestra di dialogo della capacità e della posizione del disco.

13. Specificare la capacità e la posizione del disco e fare clic su Avanti. Verrà visualizzata la finestra di dialogo opzioni avanzate.

    È possibile archiviare il disco con la macchina virtuale o specificare un'altra posizione. Si consiglia un minimo di 500 GB.

14. Accettare i valori predefiniti per le Opzioni avanzate e fare clic su Avanti.
15. Confermare le impostazioni e fare clic su Fine per creare la nuova macchina virtuale.

Aggiunta di unità disco virtuali

Utilizzare questa procedura per aggiungere unità disco virtuali per l'archiviazione dei registri eventi. Utilizzare le stesse impostazioni a prescindere dal ruolo che un server CA Enterprise Log Manager specifico svolge all'interno della rete.

Per modificare le impostazioni

1. fare clic con il pulsante destro sulla macchina virtuale in VMware Infrastructure Client e selezionare Modifica impostazioni.

   Verrà visualizzata la finestra di dialogo Proprietà macchina virtuale.

2. Evidenziare le proprietà dell'Unità CD/DVD 1.
3. Fare clic sul pulsante di opzione Periferica host e selezionare l'unità DVD-ROM dall'elenco a discesa.
4. Selezionare l'opzione Stato periferica, Connetti all'accensione.
5. Fare clic su Aggiungi per avviare l'Aggiunta hardware guidato e aggiungere un secondo disco rigido.
6. Evidenziare il disco rigido nell'elenco delle periferiche e fare clic su Avanti. Verrà visualizzata la finestra di dialogo Selezionare un disco.
7. Selezionare l'opzione Crea nuovo disco virtuale e fare clic su Avanti.

8. Specificare le dimensioni del nuovo disco e selezionare l'opzione Specificare un datastore per impostarne la posizione.

   CA Enterprise Log Manager rileva questa periferica aggiuntiva durante l'installazione e l'assegna all'archiviazione dei dati. Si consiglia di massimizzare la quantità di archiviazione da rendere disponibile per CA Enterprise Log Manager.

   Nota: l'impostazione Dimensione blocco in VMware ESX Server è 1 MB; ciò limita lo spazio massimo su disco che è possibile creare a 256 GB. Se è necessario più spazio, fino a 512 GB, aumentare l'impostazione Dimensione blocco a 2 MB utilizzando questo comando:

   ```
   Vmkfstools --createfs vmfs3 --blocksize 2M vmhba0:0:0:3
   ```

   Per rendere effettive le nuove impostazioni è necessario riavviare ESX Server. Ulteriori informazioni su questo e altri comandi sono disponibili nella documentazione di VMware ESX Server.

   fare clic su Avanti per visualizzare la finestra di dialogo Specificare opzioni avanzate.

9. Accettare i valori predefiniti per le Opzioni avanzate e fare clic su Avanti. Comparirà la finestra di dialogo Pronto per il completamento.

10. Fare clic su Fine per archiviare le modifiche a questa macchina virtuale. Questa azione restituisce la finestra di dialogo di VMware Infrastructure Client.

Installare CA Enterprise Log Manager sulla macchina virtuale

Utilizzare questa procedura per installare CA Enterprise Log Manager su una macchina virtuale creata in precedenza.

È possibile configurare un server CA Enterprise Log Manager virtuale o dedicato dopo l'installazione affinché svolga uno di diversi ruoli funzionali come gestione, raccolta o rapporti. Se si installa un server di gestione CA Enterprise Log Manager, non utilizzarlo per ricevere i registri eventi o per eseguire query e rapporti. Installare server virtuali CA Enterprise Log Manager separati che operino come server di rapporto e di raccolta per ottenere le prestazioni migliori.

Rivedere le istruzioni dell'installazione normale prima di installare CA Enterprise Log Manager in un ambiente virtuale. Il foglio di calcolo dell'installazione aiuta a raccogliere le informazioni necessarie.

Per installare CA Enterprise Log Manager in una macchina virtuale

1. Caricare il disco di installazione del SO CA Enterprise Log Manager nell'unità DVD-ROM fisica o localizzare la directory in cui è stata copiata l'immagine di installazione.
2. Evidenziare la macchina virtuale nell'elenco dell'inventario delle macchine virtuali, fare clic con il pulsante destro su di essa e selezionare Accendi.
3. Procedere con l'installazione normale di CA Enterprise Log Manager.
4. Configurare il server CA Enterprise Log Manager installato per il ruolo funzionale richiesto, utilizzando le informazioni nella sezione sull'installazione di un server CA Enterprise Log Manager.

Ulteriori informazioni

Installazione di CA Enterprise Log Manager (a pagina 85)

Clonazione di un server CA Enterprise Log Manager virtuale

È possibile utilizzare questa procedura per clonare un server CA Enterprise Log Manager virtuale. Questa procedura presume che sia già stata creata una nuova macchina virtuale, che a questa siano state aggiunte le unità disco e che CA Enterprise Log Manager sia stato installato.

Duplicazione di un server virtuale

1. Accedere a VMware VirtualCenter e individuare la macchina virtuale che contiene CA Enterprise Log Manager.
2. Disattivare la macchina virtuale se è in funzione.
3. Selezionare l'opzione Esporta e definire un percorso per la macchina virtuale esportata.

   Il server VMware ESX offre dei metodi alternativi per la clonazione di macchine virtuali. Per ulteriori informazioni, consultare la documentazione VMware.

Importazione di una macchina virtuale clonata a un server di destinazione

Utilizzare questa procedura per importare una macchina virtuale clonata su un altro server per l'attivazione.

Importazione di una macchina virtuale clonata

1. Verificare di disporre dell'accesso di rete al server host di destinazione.
2. Accedere a VMware VirtualCenter dal server che ospita VMware ESX.
3. Selezionare l'opzione Importa e quindi individuare il server di destinazione rispondendo ai prompt supplementari come richiesto.

   L'azione di importazione sposta la macchina virtuale clonata sul server di destinazione. La documentazione di VMware ESX contiene ulteriori informazioni.

Aggiornamento di un serverCA Enterprise Log Manager clonato prima della distribuzione

Utilizzare questa procedura per aggiornare un server virtuale CA Enterprise Log Manager clonato.

Un server virtuale CA Enterprise Log Manager clonato conserva il nome dell'host assegnato durante l'installazione. Tuttavia, il nome dell'host per ciascun server CA Enterprise Log Manager attivo deve essere univoco all'interno dell'implementazione della raccolta registri. Quindi, prima di poter attivare un server virtuale clonato, modificare il nome dell'host e l'indirizzo IP del server con lo script *Rename_ELM.sh*.

Lo script di aggiornamento esegue azioni che comprendono:

- Arresto automatico e riavvio dell'agente predefinito
- Arresto automatico e riavvio del servizio iGateway
- Richiesta di modifica di nome host, indirizzo IP e indirizzo IP DNS
- Aggiornamento automatico dei file di configurazione con password crittografate per i diversi certificati

Per aggiornare un server CA Enterprise Log Manager virtuale clonato

1. Accedere al server fisico di destinazione come root.
2. Aprire l'immagine ISO o il DVD dell'applicazione e accedere alla directory, /CA/Linux_x86.

   Lo script è disponibile anche nel file system di un server CA Enterprise Log Manager installato. Lo script risiede nella directory opt/CA/LogManager.
3. Copiare lo script Rename_ELM.sh nel server di destinazione.
4. Modificare le informazioni per il server CA Enterprise Log Manager virtuale con il comando seguente:

   ```
   ./Rename_ELM.sh
   ```
5. Rispondere ai prompt.
6. Avviare la macchina virtuale che contiene il server virtuale aggiornato.

Creazione di server CA Enterprise Log Manager mediante applicazioni virtuali

CA Enterprise Log Manager può essere distribuito come applicazione virtuale in formato Open Virtualization Format (OVF). Il provisioning di applicazioni virtuali richiede meno tempo dell'installazione o clonazione di un server CA Enterprise Log Manager su un computer virtuale.

Informazioni sulle applicazioni virtuali CA Enterprise Log Manager

OVF è uno standard aperto per la creazione e la distribuzione di applicazioni virtuali. CA Enterprise Log Manager utilizza il formato file VMDK (Virtual Machine Disk) basato sul formato OVF. Il pacchetto OVF contiene i seguenti file:

File XML del descrittore OVF

Un file XML del descrittore OVF con estensione .ovf. Il file contiene le specifiche dell'hardware virtuale, i parametri di configurazione di CA Enterprise Log Manager e il contratto di licenza.

File di disco virtuale

I file di disco virtuale VMware vSphere, che contengono file di immagine disco utilizzati per la distribuzione dell'applicazione virtuale:

- CA Enterprise Log Manager 1.vmdk
- CA Enterprise Log Manager 2.vmdk
- CA Enterprise Log Manager 3.vmdk

File manifesto

Il file CA Enterprise Log Manager.mf, che contiene la firma di tutti i file.

Nota: si consiglia di non modificare i file del disco virtuale o il file manifesto, in quanto la modifica di tali file potrebbe compromettere le prestazioni del dispositivo virtuale.

Per impostazione predefinita, il client VMware vSphere legge i dettagli importati utilizzando il modello OVF ed effettua il provisioning dell'applicazione virtuale.

Modalità di utilizzo dell'applicazione virtuale

È possibile utilizzare applicazioni virtuali per la creazione di server CA Enterprise Log Manager virtuali per il proprio ambiente di raccolta log eventi, utilizzando i seguenti scenari:

- Aggiunta di server virtuali a un ambiente CA Enterprise Log Manager esistente: creazione di un ambiente misto
- Creazione di un ambiente di raccolta log virtuale
- Distribuzione di server CA Enterprise Log Manager virtuali per una rapida scalabilità

Utilizzare il client VMware vSphere per installare l'applicazione virtuale, manualmente o in modalità invisibile. Il file del descrittore OVF contiene i parametri di configurazione per CA Enterprise Log Manager. Immettere un valore per ciascun parametro di configurazione durante l'installazione.

Foglio di lavoro per l'installazione dell'applicazione virtuale.

Prima di installare l'applicazione virtuale, raccogliere le informazioni nella tabella seguente. Una volta completato il foglio di lavoro, è possibile utilizzarlo mentre si lavora nei prompt di installazione. È possibile stampare e completare una serie di fogli di lavoro separati per ogni server CA Enterprise Log Manager che si ha intenzione di installare.

Informazioni necessarie	Valore	Commenti
Impostazioni specifiche dell'host		
Nome host	*Nome host del server CA Enterprise Log Manager* Ad esempio: CA-ELM1	Specificare il nome host del server utilizzando solo i caratteri supportati per gli host. Gli standard industriali consigliano l'utilizzo dei caratteri A-Z (senza distinzione di maiuscole), 0-9 ed i trattini, dove il primo carattere corrisponde ad una lettera e l'ultimo ad un carattere alfanumerico. Non utilizzare il trattino basso all'interno del nome host né aggiungere un nome di dominio all'host. **Nota:**: il nome host non può superare i 15 caratteri.
Password principale	*nuova password principale*	Creare e confermare una nuova password per il server.

Informazioni necessarie	Valore	Commenti
Indirizzo IP	*Indirizzo IPv4 rilevante*	Inserire un indirizzo IP valido per il server.
Subnet mask	*Indirizzo IP rilevante*	Inserire una subnet mask valida da utilizzare con il server.
Gateway predefinito	*Indirizzo IP rilevante*	Inserire un gateway predefinito valido da utilizzare con questo server.
Server DNS	*Indirizzi IPv4 corrispondenti*	Immettere uno o più indirizzi IP di server DNS utilizzati nella rete. elenco separato da virgole senza spazi tra le voci. Se i server DNS utilizzano indirizzi IPv6, immettere questi indirizzi in quel formato.
Nome dominio	*il nome del dominio*	Inserire il nome di dominio completo del server, ad esempio mycompany.com. **Nota:** per abilitare la risoluzione del nome host nell'indirizzo IP è necessario registrare il nome del dominio sul server DNS di rete.
EULA	Accetta	Leggere attentamente il contratto di licenza CA fino alla fine, quindi fare clic su Accept (Accetto) per accettare i termini del contratto.
Fuso orario	*fuso orario desiderato*	Selezionare il fuso orario del server.
Impostazioni specifiche dell'applicazione		
Posizione del server CA EEM	Locale: per il primo server installato (server di gestione) Remoto: per ogni server aggiuntivo	Indicare se si desidera utilizzare un server CA EEM locale o remoto. Per un server di gestione CA Enterprise Log Manager, scegliere il server remoto. L'installazione richiede di creare una password per l'account utente EiamAdmin predefinito. Per ogni server aggiuntivo, scegliere Remoto. L'installazione richiede il nome del server di gestione. Indipendentemente dal tipo di server scelto (locale o remoto), è necessario utilizzare l'ID e la password dell'account EiamAdmin per il primo accesso al server CA Enterprise Log Manager.

Informazioni necessarie	Valore	Commenti
Il nome host o l'indirizzo IP del server CA EEM remoto.	*Nome host o indirizzo IP*	Specificare questo valore solo se si seleziona l'opzione server remota. Immettere l'indirizzo IP o il nome host del server di gestione CA Enterprise Log Manager installato per primo. Il nome host deve essere registrato con il server DNS. Se si desidera utilizzare un server CA EEM locale, il valore predefinito è **Nessuno**.
Password del server CA EEM	*Password account EiamAdmin*	Registrare la password per l'account amministratore predefinito, EiamAdmin. L'accesso iniziale al server CA Enterprise Log Manager richiede queste credenziali dell'account. Se si installa il server di gestione, creare e confermare qui la nuova password EiamAdmin. Annotare questa password, in quanto verrà utilizzata nuovamente durante le installazioni degli altri server e agenti CA Enterprise Log Manager. **Nota**: la password immessa sarà anche la password iniziale dell'account caelmadmin predefinito utilizzato per accedere direttamente al server CA Enterprise Log Manager attraverso ssh. È possibile creare ulteriori account di amministratore per accedere alle funzioni CA EEM dopo l'installazione, se lo si desidera.
FIPS	Sì o No	Specifica se l'applicazione virtuale deve essere eseguita in modalità FIPS o non-FIPS. Se si sceglie di utilizzare un server CA EEM locale, è possibile selezionare qualsiasi modalità. Se si sceglie di utilizzare un server CA EEM remoto, è necessario selezionare la modalità utilizzata dal server remoto CA EEM.

Aggiunta di server virtuali all'ambiente

Se si dispone già di un'implementazione di CA Enterprise Log Manager, è possibile aggiungere server di raccolta CA Enterprise Log Manager per gestire un volume di eventi in aumento nella rete. Questo scenario dà per scontato che sia già stato installato un server di gestione CA Enterprise Log Manager e uno o più server CA Enterprise Log Manager per la raccolta e i rapporti.

Nota: per ottenere le migliori prestazioni, installare CA Enterprise Log Manager su server virtuali per gestire solo attività di raccolta e rapporti.

La procedura per l'aggiunta di server di raccolta virtuali all'ambiente include le seguenti procedure:

1. Download del pacchetto dell'applicazione virtuale CA Enterprise Log Manager.
2. Installazione di un server CA Enterprise Log Manager con applicazione virtuale.
3. Configurazione del server CA Enterprise Log Manager come descritto nella sezione sull'installazione.

Dopo avere installato il server di raccolta virtuale, è possibile aggiungerlo alla federazione per le query e i rapporti.

Importante: Se si desidera eseguire il provisioning di un server CA Enterprise Log Manager mediante applicazione virtuale, il nome dell'istanza applicazione del server CA Enterprise Log Manager primario deve essere CAELM.

Download del pacchetto dell'applicazione virtuale

L'immagine di distribuzione per l'applicazione virtuale CA Enterprise Log Manager è disponibile sul sito del Supporto in linea dal collegamento Download. I file da scaricare sono cinque:

- Il file manifesto
- Il file .ovf
- Tre file di disco virtuale

Installazione manuale di un server CA Enterprise Log Manager

Se si installa l'applicazione virtuale manualmente, eseguire le operazioni riportate a continuazione:

1. Distribuire un modello OVF.
2. Definire le impostazioni per la paravirtualizzazione e le risorse.
3. Attivare il server CA Enterprise Log Manager di cui è stato eseguito il provisioning.

Distribuire un modello OVF

È possibile specificare le proprietà dell'applicazione virtuale in un modello OVF. VMware utilizza questo modello per eseguire il provisioning di un server CA Enterprise Log Manager. Utilizzare il client VMware vSphere per eseguire la distribuzione del modello OVF.

Nota: le catture di schermata riportate nelle procedure seguenti contengono dati di esempio. Le catture di schermata riportate fanno riferimento al client VMware vSphere 4.0.0. Si raccomanda di specificare dati consoni al proprio ambiente.

Per distribuire un modello OVF:

1. Fare clic su Start, Programmi, VMware vSphere Client sul computer su cui è installato il client VMware vSphere.

   Viene visualizzata la finestra di dialogo del client VMware vSphere.

2. Nel campo relativo all'indirizzo IP/nome host, immettere l'indirizzo IP o il nome host del server VMware vSphere a cui si desidera effettuare la connessione.
3. Immettere le credenziali di accesso nei campi Nome utente e Password.
4. Fare clic su Logon (Accedi).

   Viene visualizzata la finestra dell'applicazione.

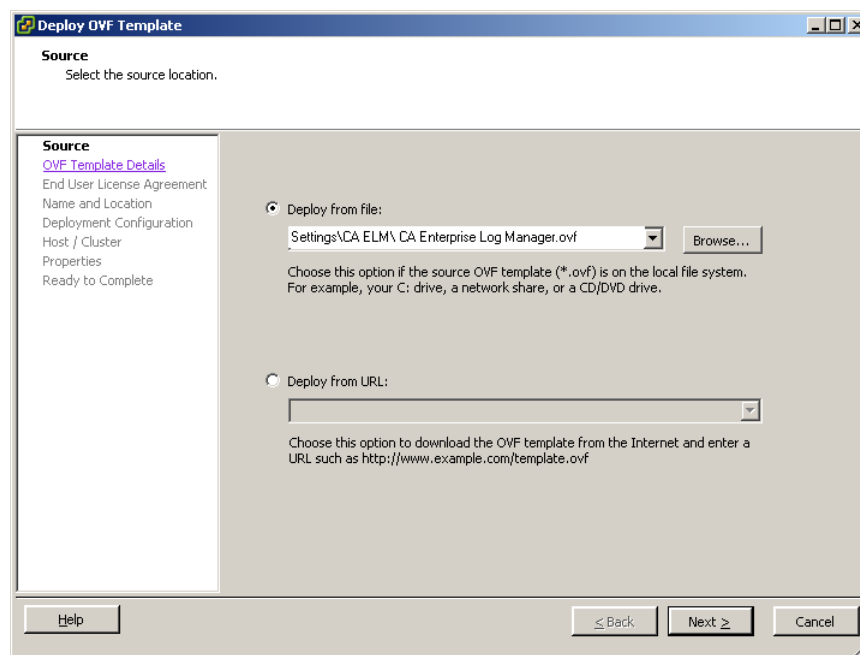
5. Selezionare la posizione in cui si desidera eseguire il provisioning del server CA Enterprise Log Manager sotto un centro dati del riquadro sinistro.
6. Fare clic su File, quindi sull'opzione di distribuzione del modello OVF.

   Viene visualizzata la finestra di distribuzione del modello OVF. Per impostazione predefinita, la finestra di distribuzione del modello OVF visualizza la pagina di origine. Immettere la posizione del modello OVF in questa pagina.

   Nota: le pagine visualizzate nella finestra di distribuzione del modello OVF variano in base alla versione e alle impostazioni del client VMware vSphere in uso. Per ulteriori informazioni sulla distribuzione di un modello OVF, visitare il sito www.vmware.com.

7. Scegliere l'opzione Deploy from file (Distribuisci da file) e fare clic su Sfoglia per selezionare la posizione del modello OVF.
8. Raggiungere la posizione del modello OVF dalla finestra di dialogo Open (Apri), selezionare il modello OVF, quindi fare clic su Apri.

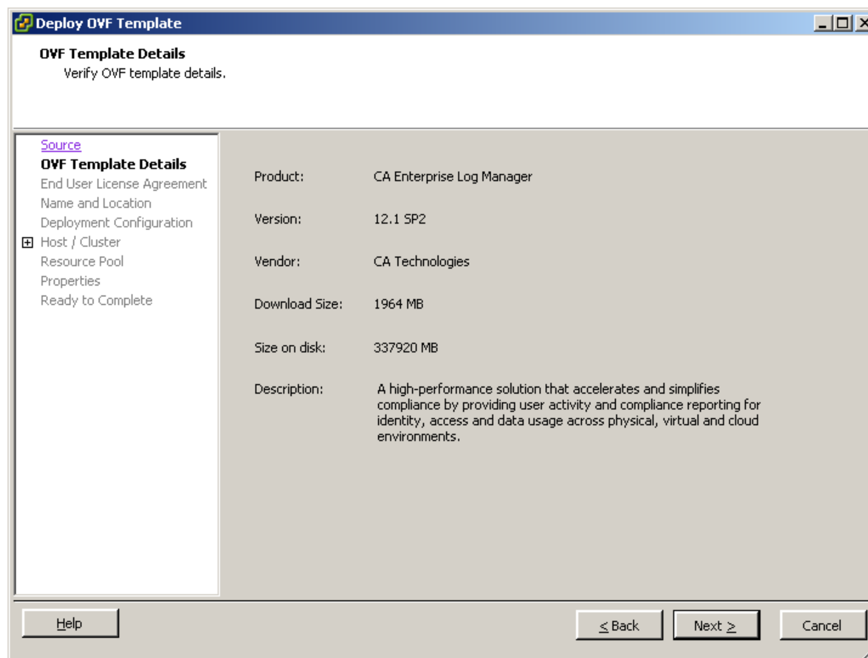
   Il percorso della posizione del modello OVF viene visualizzato nel campo Deploy from file.



9. Fare clic su Avanti.

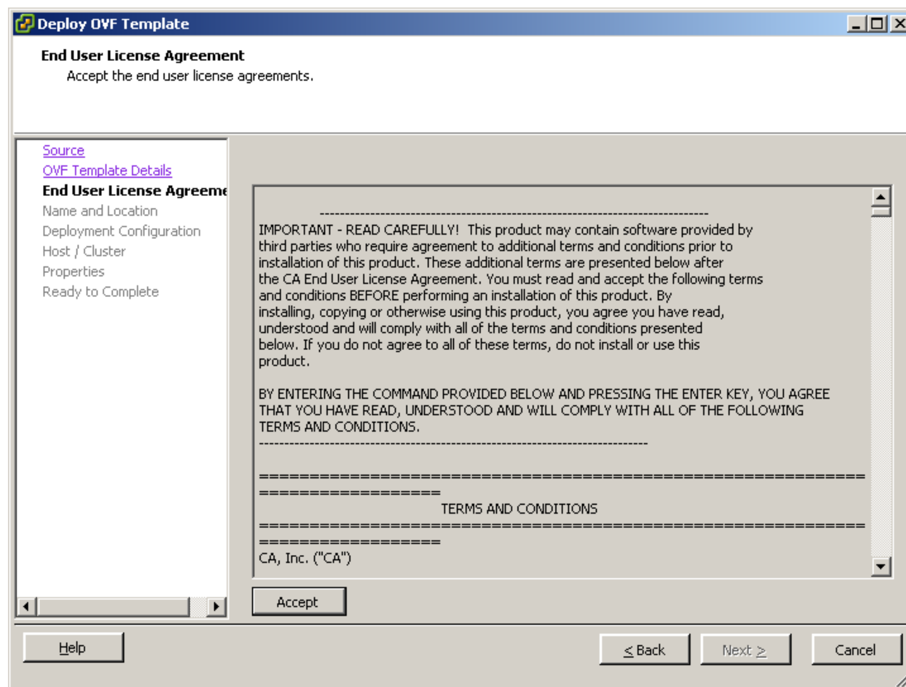
   Viene visualizzata la pagina dei dettagli del modello OVF. La pagina consente di visualizzare i dettagli archiviati nel modello OVF, quali le dimensioni di download, lo spazio su disco disponibile e il nome del fornitore.

10. Verificare di disporre di un minimo di 350 GB di spazio su disco sul server VMware, quindi fare clic su Avanti.



Viene visualizzata la pagina del contratto di licenza per l'utente finale. In questa pagina viene visualizzato il contratto di licenza per i prodotti di terze parti. Sarà necessario accettare il contratto di licenza per poter procedere all'installazione di CA Enterprise Log Manager.

11. Leggere il testo del contratto.

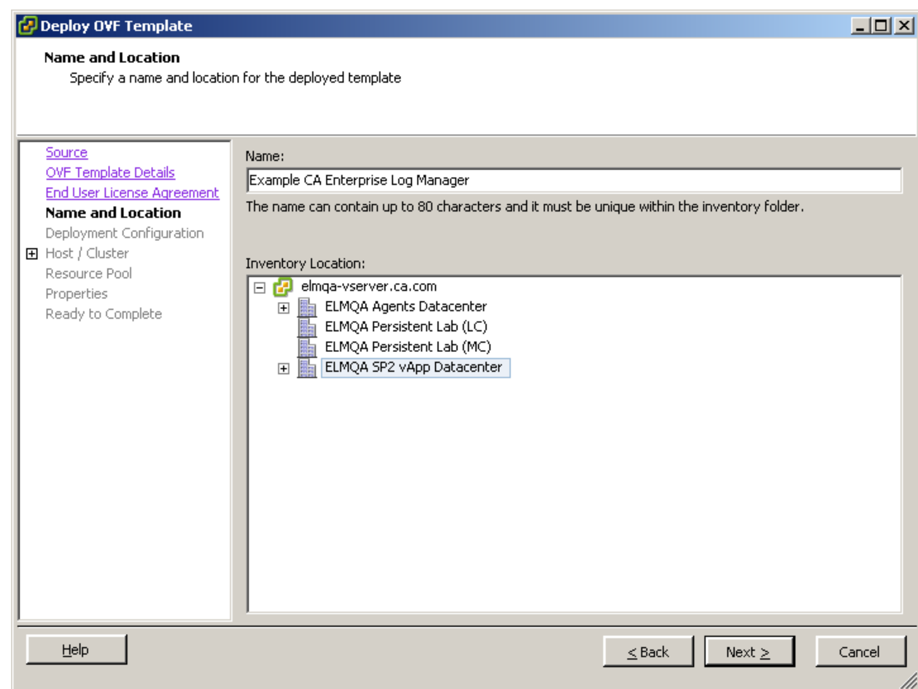


12. Accettare i termini del contratto, quindi fare clic su Avanti.

    Verrà visualizzata la pagina relativa al nome e alla posizione. In questa pagina sarà possibile indicare un nome per identificare il server CA Enterprise Log Manager e specificare il centro dati in cui si desidera eseguire il provisioning del server CA Enterprise Log Manager.

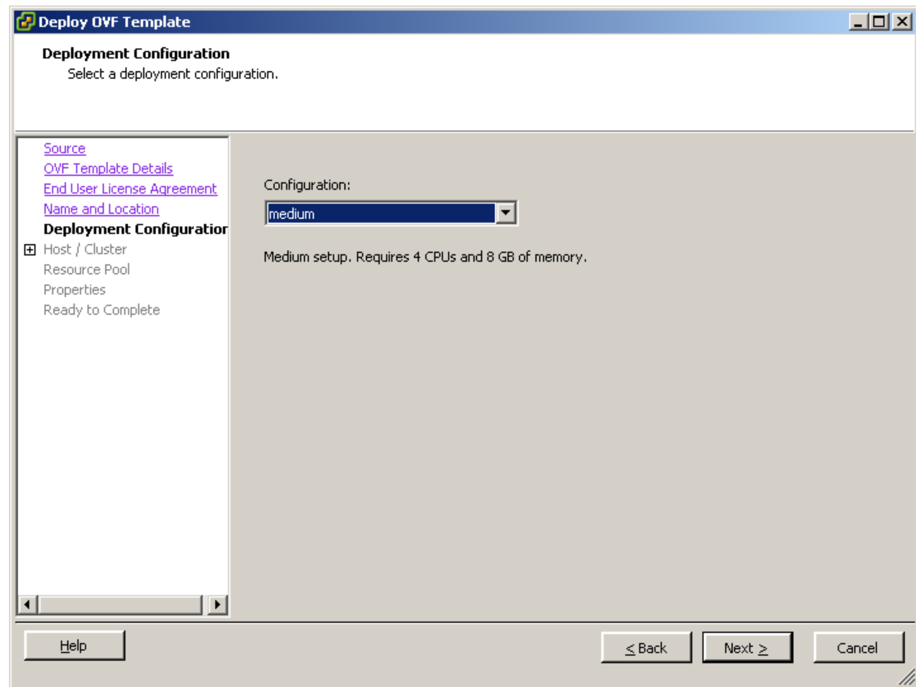
13. Immettere il nome del server CA Enterprise Log Manager nel campo Nome, selezionare il centro dati da Inventory Location (Posizione inventario), quindi fare clic su Avanti.

    Nota: per impostazione predefinita, il nome specificato nel modello OVF viene visualizzato nel campo Nome.



Viene visualizzata la pagina di configurazione della distribuzione. La pagina della configurazione di distribuzione consente di specificare la modalità di configurazione del serverCA Enterprise Log Manager di cui si desidera effettuare il provisioning.

14. Dal menu a discesa Configurazione, selezionare Medium (Media) o Large (Estesa), quindi fare clic su Avanti.

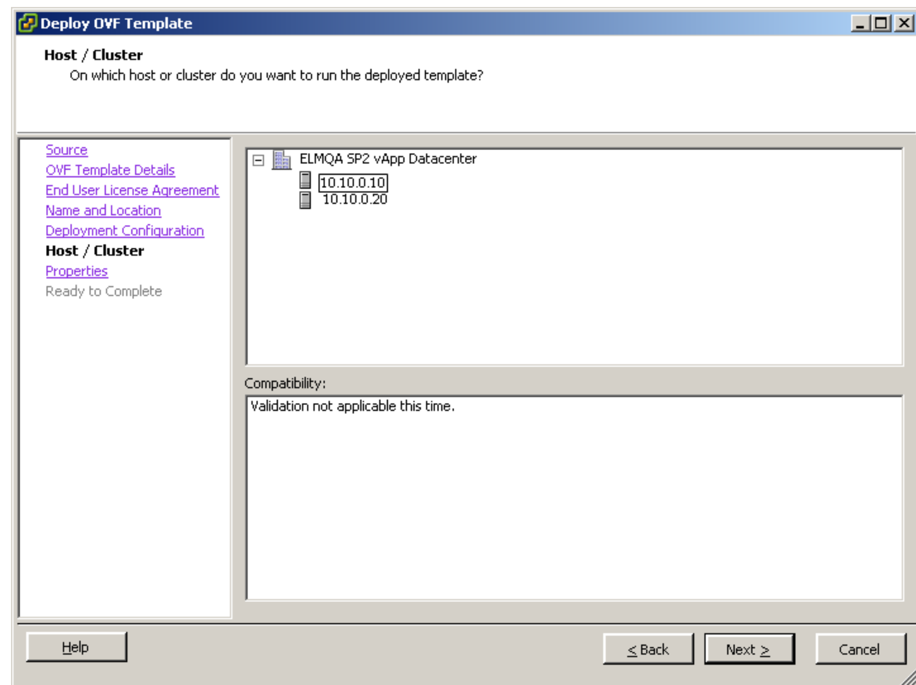


Se si seleziona Media, VMware indica quattro CPU con 8 GB di RAM ciascuna. Se si seleziona Estesa, VMware indica otto CPU con 8 GB di RAM ciascuna.

Nota: si consiglia di utilizzare una configurazione di distribuzione media per effettuare il provisioning di un server di raccolta e una configurazione di distribuzione estesa per effettuare il provisioning di un server di gestione o di rapporto.

Si aprirà la pagina Host/Cluster. Questa pagina viene visualizzata solo se non è stato selezionato il pool di risorse prima di avviare l'importazione del modello OVF. La pagina Host/Cluster visualizza il centro dati selezionato e i cluster disponibili. È necessario specificare la posizione del cluster nel centro dati in cui si desidera eseguire il provisioning del server CA Enterprise Log Manager.

15. Selezionare un cluster nel centro dati, quindi fare clic su Avanti.



Viene visualizzata la pagina delle proprietà. Questa pagina contiene le impostazioni dell'host e di CA Enterprise Log Manager.

16. Immettere i valori per ciascun campo utilizzando le informazioni raccolte nel foglio di lavoro di installazione, quindi fare clic su Avanti.

Deploy OVF Template

Properties

Customize the software solution for this deployment.

Source
OVF Template Details
End User License Agreement
Name and Location
Deployment Configuration
Host / Cluster
Resource Pool
Properties
Ready to Complete

B. CA Enterprise Log Manager Settings

A. Location of CA EEM Server

Select Local if the CA EEM server is to be installed on this host. Select Remote if this CA Enterprise Log Manager server must use a remote CA EEM server.

Local

B. Host Name or IP Address of the Remote CA EEM Server

Specify the IP address or the host name of the remote CA EEM server. Enter none to install a CA EEM server on this host.

none

C. Password for CA EEM Server

Enter the password for the EEM server EiamAdmin user.

exampleeiamadminpassword

D. FIPS Mode

Do you want to run CA Enterprise Log Manager in FIPS mode? Choose Yes for FIPS mode or No for non-FIPS mode.

NO

Help | < Back | Next > | Cancel

Viene visualizzata la pagina Ready to Complete (Pronto per il completamento). La pagina visualizza un riepilogo delle informazioni immesse nelle pagine precedenti.

17. Verificare le informazioni immesse, quindi fare clic su Fine.

Deploy OVF Template

Ready to Complete

Are these the options you want to use?

Source
OVF Template Details
End User License Agreement
Name and Location
Deployment Configuration
Host / Cluster
Properties
Ready to Complete

When you click Finish, the deployment task will be started.

Deployment settings:

OVF file:	C:\Program Files\CA ELM\CA Enterprise Log Manager.ovf
Download Size:	1964 MB
Size on disk:	337920 MB
Name:	Example CA Enterprise Log Manager
Folder:	ELMQA SP2 vApp Datacenter
Deployment Configuration:	medium
Host/Cluster:	10.10.0.10
Datastore:	Storage - 172.60.10.20
Network Mapping:	"VM Network" to "VM Network"
IP Allocation:	Fixed, IPv4
Property:	HOSTNAME = examplecaelm
Property:	ROOT_PASSWORD = examplerootpassword
Property:	IP_ADDRESS = 172.60.0.0
Property:	SUBNET_MASK = 10.0.0.0
Property:	DEFAULT_GATEWAY = 198.168.0.0
Property:	DNS_SERVERS = 198.168.10.20, 198.168.10.25
Property:	DOMAIN_NAME = example.com
Property:	TIMEZONE = Africa/Abidjan
Property:	LOCAL_REMOTE_EEM = Local
Property:	REMOTE_EEM_LOCATION = none
Property:	EEM_PASSWORD = exampleeiamadminpassword
Property:	FIPS_MODE = YES
Property:	AGENT_AUTHENTICATION_KEY = This_is_default_authentication_key

Help | < Back | Finish | Cancel

Viene visualizzato il messaggio Opening VI target (Apertura destinazione VI in corso...) Viene visualizzato lo stato di distribuzione dell'applicazione virtuale. Se l'installazione viene completata correttamente, l'applicazione virtuale viene visualizzata nel centro dati selezionato nel riquadro sinistro.

18. (Facoltativo) Se si desidera modificare le informazioni immesse, eseguire le seguenti operazioni:

    a. Nella finestra relativa alla distribuzione del modello OVF, fare clic ripetutamente su Indietro fino a raggiungere la pagina da modificare.

    b. Apportare le modifiche necessarie.

    c. Quindi, fare clic ripetutamente su Avanti fino a raggiungere la pagina Ready to Complete (Pronto per il completamento).

Definizione delle impostazioni per la paravirtualizzazione e le risorse

Dopo aver importato il modello OVF, è necessario definire manualmente le impostazioni della paravirtualizzazione e delle risorse per migliorare le prestazioni del server CA Enterprise Log Manager di cui è stato eseguito il provisioning.

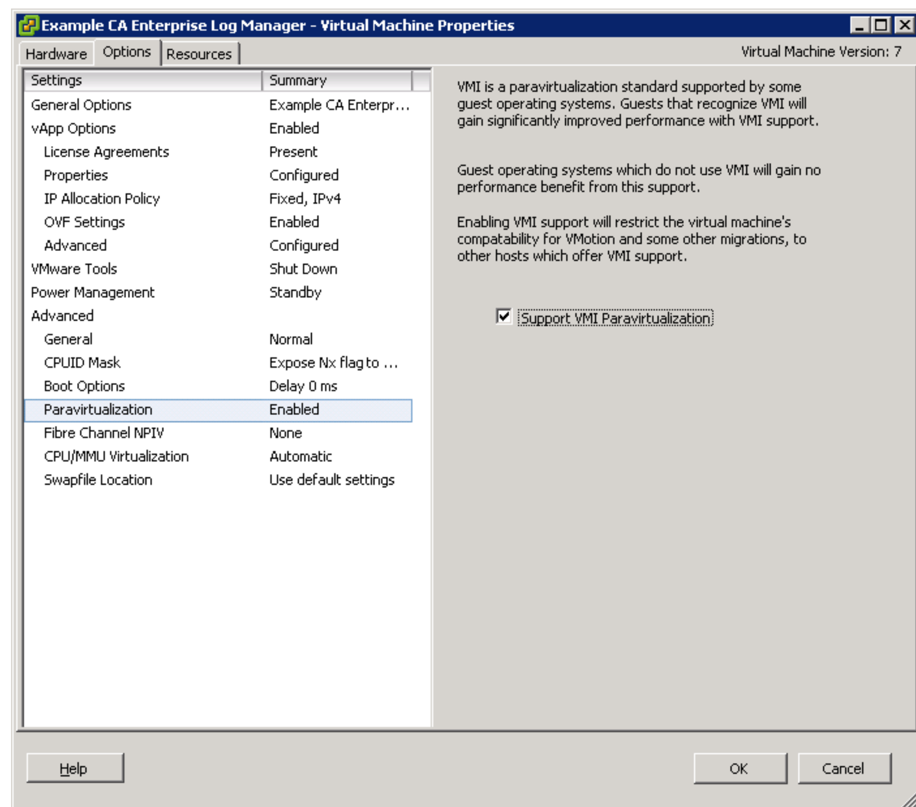
Per definire le impostazioni della paravirtualizzazione e delle risorse:

1. Fare clic con il pulsante destro del mouse sulla nuova applicazione virtuale di CA Enterprise Log Manager nel riquadro sinistro, quindi sull'opzione di modifica impostazioni.

   Viene visualizzata la finestra <*CA Enterprise Log Manager Virtual Appliance name*> - Virtual Machine Properties (Proprietà del computer virtuale <CA Enterprise Log Manager Virtual Appliance name>)

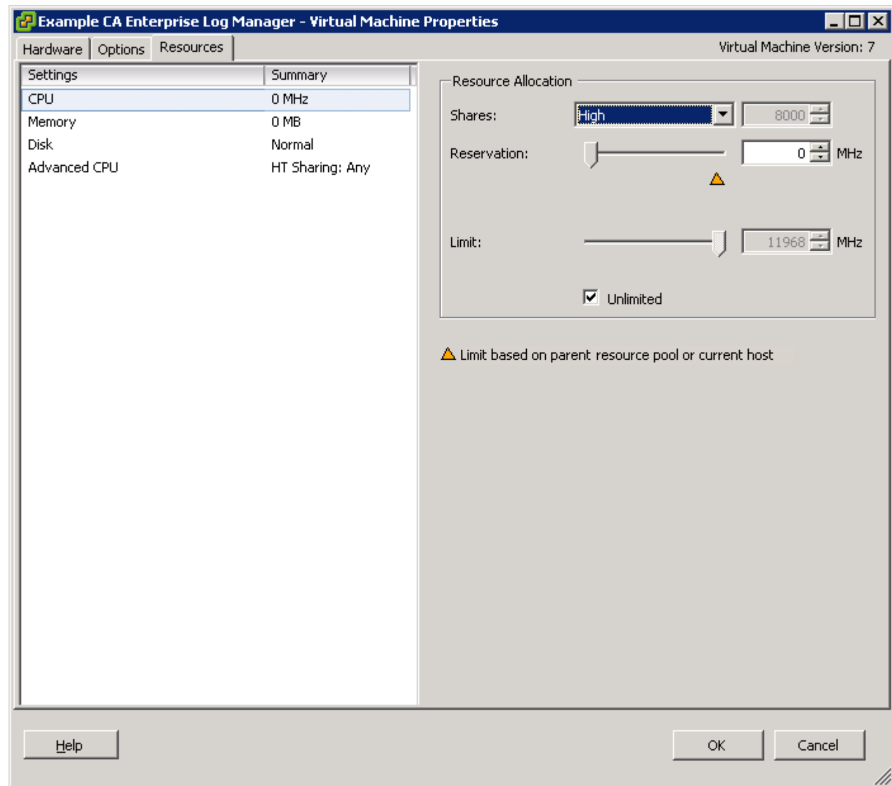
2. Fare clic sulla scheda Opzioni.

3. Selezionare l'impostazione di paravirtualizzazione nel riquadro sinistro quindi l'opzione per il supporto della paravirtualizzazione VMI nel riquadro destro.

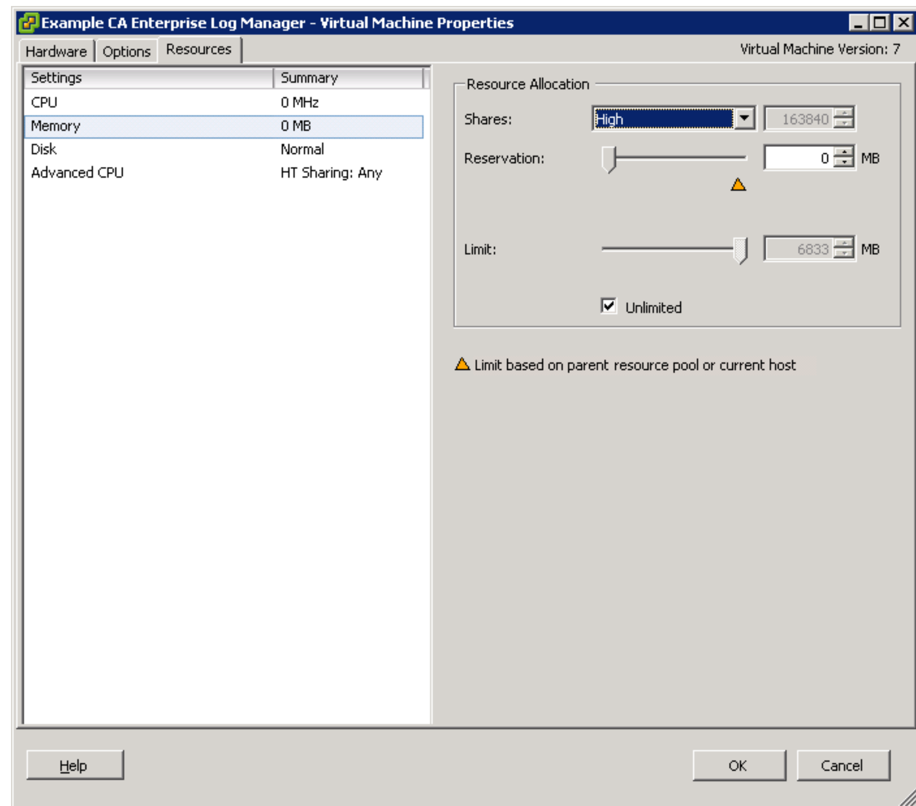


4. Fare clic sulla scheda Risorse.

5. Selezionare l'opzione CPU nella colonna Impostazioni, quindi selezionare High (Alta) dal menu a discesa Shares (Condivisioni) nella sezione Resource allocation (Allocazione risorse).



6. Selezionare l'opzione Memory (Memoria) nella colonna Impostazioni, quindi selezionare High (Alta) dal menu a discesa Shares (Condivisioni) nella sezione Resource allocation (Allocazione risorse).



7. Fare clic su OK.

8. **Nota**: per ulteriori informazioni sulla paravirtualizzazione, si rimanda al sito www.vmware.com.

Attivare il server CA Enterprise Log Manager di cui è stato eseguito il provisioning.

Il server CA Enterprise Log Manager deve essere attivato per poter dare inizio all'esecuzione.

Per attivare un server CA Enterprise Log Manager:

1. Selezionare il nuovo server CA Enterprise Log Manager nel riquadro sinistro della finestra dell'applicazione VMware.
2. Fare clic sull'opzione di avvio in Basic Tasks (Attività di base) della scheda Getting Started (Introduzione) del riquadro destro.

   Il server CA Enterprise Log Manager verrà attivato.

Nota: verificare che un server primario CA Enterprise Log Manager sia in esecuzione prima di attivare un server secondario CA Enterprise Log Manager.

Installazione invisibile di un server CA Enterprise Log Manager

Quando si procede all'installazione dell'applicazione virtuale in modalità invisibile all'utente, è necessario eseguire le seguenti operazioni:

1. Richiamare lo strumento OVF.
2. Definire le impostazioni per la paravirtualizzazione e le risorse.
3. Attivare il server CA Enterprise Log Manager di cui è stato eseguito il provisioning.

La tabella seguente descrive i parametri utilizzati per eseguire la distribuzione di CA Enterprise Log Manager mediante lo strumento OVF. È necessario specificare tali parametri come argomenti della riga di comando.

Informazioni necessarie	Valore	Commenti
Impostazioni specifiche dell'host		

Informazioni necessarie	Valore	Commenti
HOSTNAME	*Nome host del server CA Enterprise Log Manager* Ad esempio: CA-ELM1	Specificare il nome host del server utilizzando solo i caratteri supportati per gli host. Gli standard industriali consigliano l'utilizzo dei caratteri A-Z (senza distinzione di maiuscole), 0-9 ed i trattini, dove il primo carattere corrisponde ad una lettera e l'ultimo ad un carattere alfanumerico. Non utilizzare il trattino basso all'interno del nome host né aggiungere un nome di dominio all'host. **Nota:**: il nome host non può superare i 15 caratteri.
ROOT_PASSWORD	*nuova password principale*	Creare e confermare una nuova password per il server.
IP_ADDRESS	*Indirizzo IPv4 rilevante*	Inserire un indirizzo IP valido per il server.
SUBNET_MASK	*Indirizzo IP rilevante*	Inserire una subnet mask valida da utilizzare con il server.
DEFAULT_GATEWAY	*Indirizzo IP rilevante*	Inserire una subnet mask ed un gate predefinito da utilizzare con il server.
DNS_SERVERS	*Indirizzi IPv4 corrispondenti*	Immettere uno o più indirizzi IP di server DNS utilizzati nella rete. elenco separato da virgole senza spazi tra le voci. Se i server DNS utilizzano indirizzi IPv6, immettere questi indirizzi in quel formato.
DOMAIN_NAME	*il nome del dominio*	Inserire il nome di dominio completo del server, ad esempio mycompany.com. **Nota:** per abilitare la risoluzione del nome host nell'indirizzo IP è necessario registrare il nome del dominio sul server DNS di rete.
acceptAllEulas	Accetta	Accettare il contratto di licenza di CA per procedere con il provisioning del server CA Enterprise Log Manager.
deploymentOption	medium (media) o large (estesa).	Se si seleziona Media, VMware indica quattro CPU con 8 GB di RAM ciascuna. Se si seleziona Estesa, VMware indica otto CPU con 8 GB di RAM ciascuna.

Informazioni necessarie	Valore	Commenti
TIMEZONE	*fuso orario desiderato*	Selezionare il fuso orario del server.
Impostazioni specifiche dell'applicazione		
LOCAL_REMOTE_EEM	Locale: per il primo server installato (server di gestione) Remoto: per ogni server aggiuntivo	Indicare se si desidera utilizzare un server CA EEM locale o remoto. Per un server di gestione CA Enterprise Log Manager, scegliere il server remoto. L'installazione richiede di creare una password per l'account utente EiamAdmin predefinito. Per ogni server aggiuntivo, scegliere Remoto. L'installazione richiede il nome del server di gestione. Indipendentemente dal tipo di server scelto (locale o remoto), è necessario utilizzare l'ID e la password dell'account EiamAdmin per il primo accesso al server CA Enterprise Log Manager.
REMOTE_EEM_LOCATION	*Nome host o indirizzo IP*	Specificare questo valore solo se si seleziona l'opzione server remota. Immettere l'indirizzo IP o il nome host del server di gestione CA Enterprise Log Manager installato per primo. Il nome host deve essere registrato con il server DNS. Se si desidera utilizzare un server CA EEM locale, il valore predefinito è **Nessuno**.

Informazioni necessarie	Valore	Commenti
EEM_PASSWORD	*Password account EiamAdmin*	Registrare la password per l'account amministratore predefinito, EiamAdmin. L'accesso iniziale al server CA Enterprise Log Manager richiede queste credenziali dell'account. Se si installa il server di gestione, creare e confermare qui la nuova password EiamAdmin. Annotare questa password, in quanto verrà utilizzata nuovamente durante le installazioni degli altri server e agenti CA Enterprise Log Manager. **Nota**: la password immessa sarà anche la password iniziale dell'account caelmadmin predefinito utilizzato per accedere direttamente al server CA Enterprise Log Manager attraverso ssh. È possibile creare ulteriori account di amministratore per accedere alle funzioni CA EEM dopo l'installazione, se lo si desidera.
FIPS_MODE	Sì o No	Specifica se l'applicazione virtuale deve essere eseguita in modalità FIPS o non-FIPS. Se si sceglie di utilizzare un server CA EEM locale, è possibile selezionare qualsiasi modalità. Se si sceglie di utilizzare un server CA EEM remoto, è necessario selezionare la modalità utilizzata dal server remoto CA EEM.

Ulteriori informazioni

Aggiunta di server virtuali all'ambiente (a pagina 325)
Creazione di un ambiente completamente virtuale (a pagina 348)
Distribuzione rapida di server virtuali (a pagina 373)

Richiamare lo strumento OVF dalla riga di comando

Nota: è necessario installare lo strumento OVF 1.0.0.0 prima di eseguire l'installazione invisibile all'utente. Per ulteriori informazioni sullo strumento OVF, consultare la *Guida per l'utente dello strumento OVF* oppure visitare il sito www.vmware.com.

Per richiamare lo strumento OVF, è necessario passare i parametri di configurazione come argomenti della riga di comando.

Nota: si consiglia di utilizzare una configurazione di distribuzione media per effettuare il provisioning di un server di raccolta e una configurazione di distribuzione estesa per effettuare il provisioning di un server di rapporto. È consigliabile anche utilizzare il metodo di distribuzione thick come descritto nella documentazione VMware.

Per richiamare lo strumento OVF dalla riga di comando:

1. Aprire il prompt dei comandi sul computer in cui è installato VMware vSphere Client.
2. Per richiamare lo strumento OVF, eseguire il seguente comando:

```
ovftool -dm=thick --acceptAllEulas --name=value --deploymentOption=value --
prop:ROOT_PASSWORD=value --prop:LOCAL_REMOTE_EEM=value --
prop:REMOTE_EEM_LOCATION=value --prop:EEM_PASSWORD=value --
prop:FIPS_MODE=value --prop:IP_ADDRESS=value --prop:SUBNET_MASK=value --
prop:HOSTNAME=value --prop:DEFAULT_GATEWAY=value --prop:DNS_SERVERS=value --
prop:DOMAIN_NAME=value --prop:TIMEZONE=value <OVF_Name.ovf>
vi://username:password@hostname_of_VMware_vSphere_Client/Datacenter/host/host
name
```

   Viene visualizzato il messaggio Opening VI target (Apertura destinazione VI in corso...) Viene visualizzato lo stato di distribuzione del server CA Enterprise Log Manager. Se l'installazione viene completata correttamente, il server CA Enterprise Log Manager viene visualizzata nel centro dati selezionato nel riquadro sinistro.

   Note: se il valore di una proprietà contiene spazi, racchiudere il valore tra virgolette doppie (""). Ad esempio, se il nome OVF è CA ELM, immettere il valore come "CA ELM.ovf". Per ulteriori informazioni sullo strumento OVF, consultare la *Guida per l'utente dello strumento OVF*.

Esempio

```
ovftool -dm=thick --acceptAllEulas --name="example_server" --
deploymentOption=medium --prop:ROOT_PASSWORD="example_password" --
prop:LOCAL_REMOTE_EEM=Local --prop:REMOTE_EEM_LOCATION=none --
prop:EEM_PASSWORD=calmr12 --prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172,168.0,0 --
prop:SUBNET_MASK=10,0.0,0 --prop:HOSTNAME="example_server1" --
prop:DEFAULT_GATEWAY=198,168.0,0 --prop:DNS_SERVERS=198,168.10,20,198,168.10,25 -
-prop:DOMAIN_NAME=example.com --prop:TIMEZONE=Asia/Kolkata "C:\Program Files\CA
ELM\CA Enterprise Log Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0,10.0
"
```

Definizione delle impostazioni per la paravirtualizzazione e le risorse

Dopo aver importato il modello OVF, è necessario definire manualmente le impostazioni della paravirtualizzazione e delle risorse per migliorare le prestazioni del server CA Enterprise Log Manager di cui è stato eseguito il provisioning.

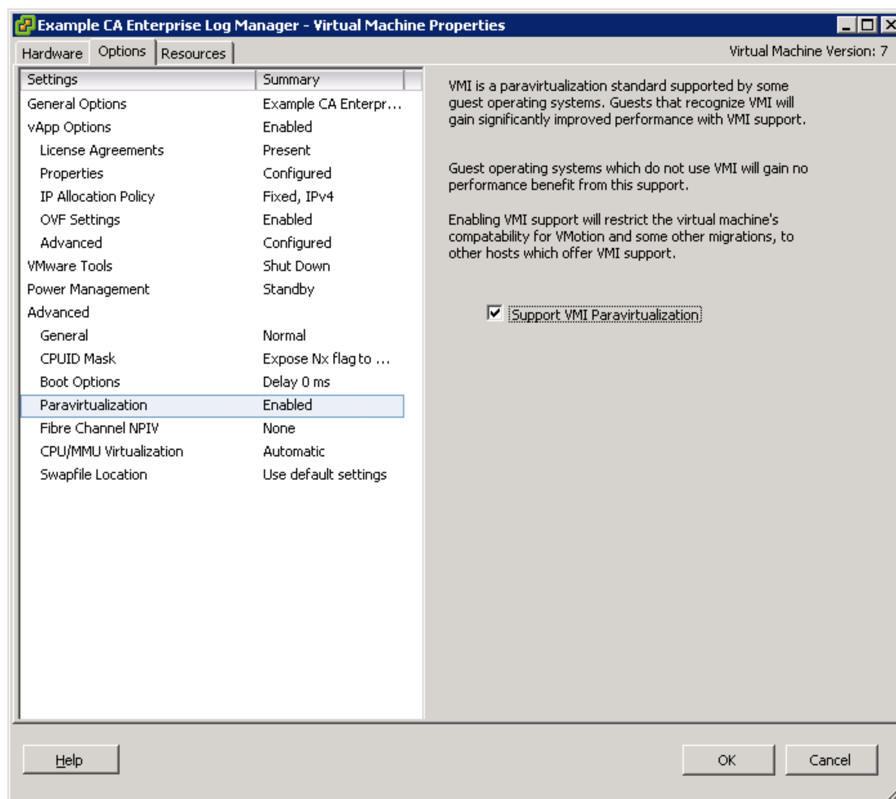
Per definire le impostazioni della paravirtualizzazione e delle risorse:

1. Fare clic con il pulsante destro del mouse sulla nuova applicazione virtuale di CA Enterprise Log Manager nel riquadro sinistro, quindi sull'opzione di modifica impostazioni.

   Viene visualizzata la finestra <*CA Enterprise Log Manager Virtual Appliance name*> - Virtual Machine Properties (Proprietà del computer virtuale <CA Enterprise Log Manager Virtual Appliance name>)

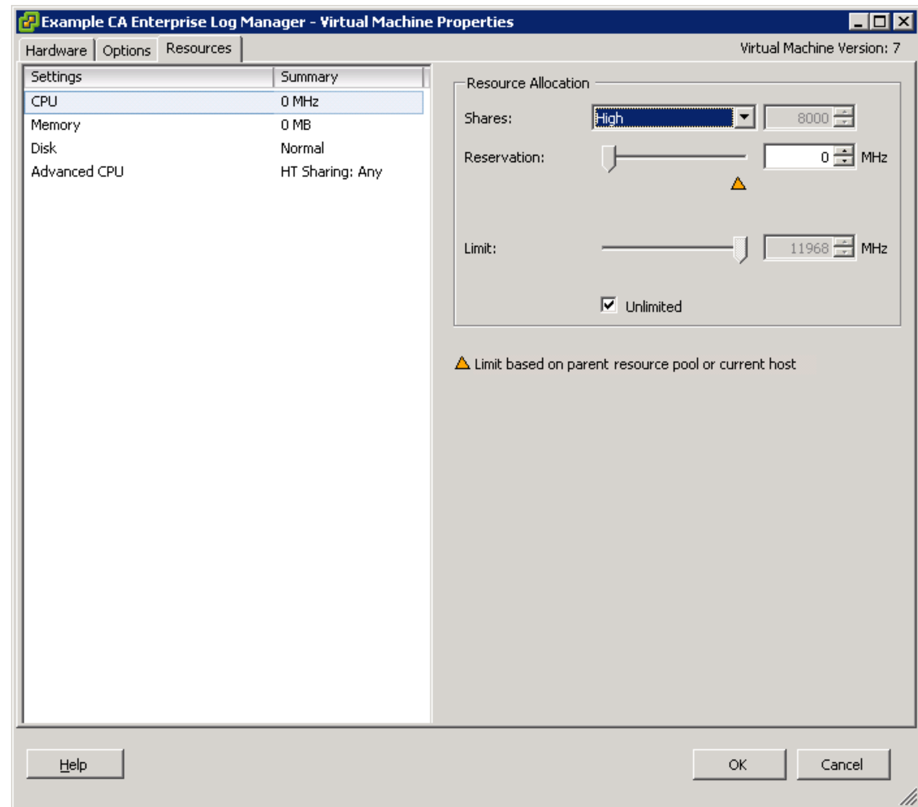
2. Fare clic sulla scheda Opzioni.

3. Selezionare l'impostazione di paravirtualizzazione nel riquadro sinistro quindi l'opzione per il supporto della paravirtualizzazione VMI nel riquadro destro.

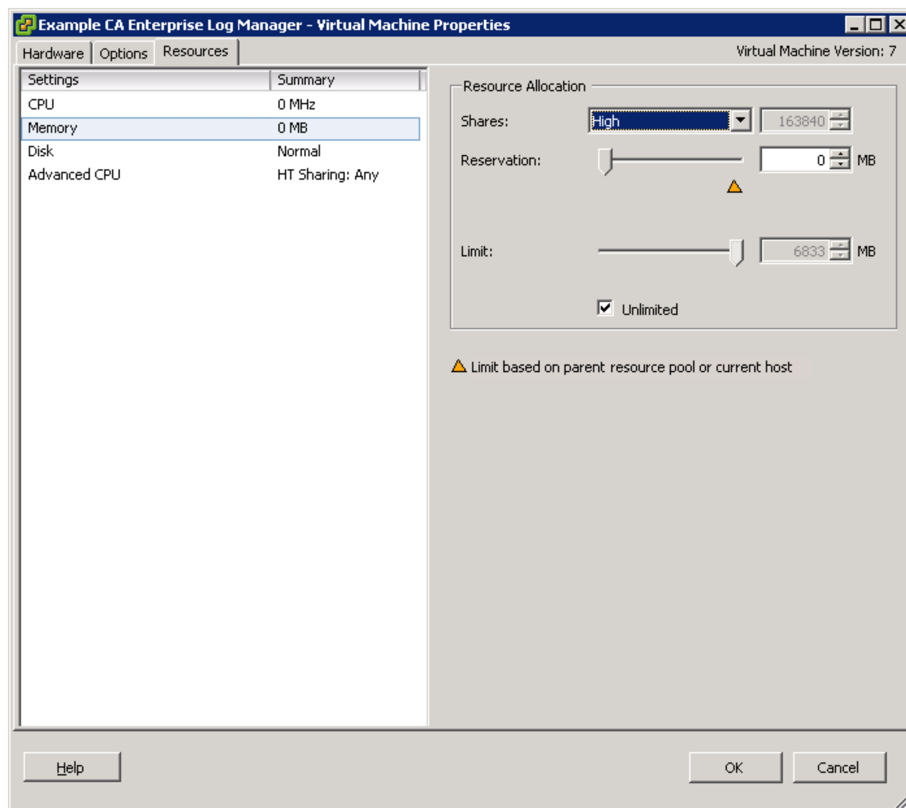


4. Fare clic sulla scheda Risorse.

5. Selezionare l'opzione CPU nella colonna Impostazioni, quindi selezionare High (Alta) dal menu a discesa Shares (Condivisioni) nella sezione Resource allocation (Allocazione risorse).



6. Selezionare l'opzione Memory (Memoria) nella colonna Impostazioni, quindi selezionare High (Alta) dal menu a discesa Shares (Condivisioni) nella sezione Resource allocation (Allocazione risorse).



7. Fare clic su OK.

8. **Nota**: per ulteriori informazioni sulla paravirtualizzazione, si rimanda al sito www.vmware.com.

Attivare il server CA Enterprise Log Manager di cui è stato eseguito il provisioning.

Il server CA Enterprise Log Manager deve essere attivato per poter dare inizio all'esecuzione.

Per attivare un server CA Enterprise Log Manager:

1. Selezionare il nuovo server CA Enterprise Log Manager nel riquadro sinistro della finestra dell'applicazione VMware.
2. Fare clic sull'opzione di avvio in Basic Tasks (Attività di base) della scheda Getting Started (Introduzione) del riquadro destro.

   Il server CA Enterprise Log Manager verrà attivato.

Nota: verificare che un server primario CA Enterprise Log Manager sia in esecuzione prima di attivare un server secondario CA Enterprise Log Manager.

Verifica dell'installazione di un server virtuale CA Enterprise Log Manager

Quando si attiva il server CA Enterprise Log Manager di cui è stato eseguito il provisioning, nella scheda della console della finestra del client VMware vSphere viene visualizzato un URL di accesso a CA Enterprise Log Manager. Utilizzare l'URL e le credenziali di accesso predefinito riportate di seguito per accedere a CA Enterprise Log Manager:

Nome utente predefinito: EiamAdmin

Password predefinita: la password immessa durante la procedura di installazione del server CA Enterprise Log Manager

Ulteriori informazioni

Aggiunta di server virtuali all'ambiente (a pagina 325)
Creazione di un ambiente completamente virtuale (a pagina 348)
Distribuzione rapida di server virtuali (a pagina 373)

Creazione di un ambiente completamente virtuale

Se non è già stato implementato un ambiente CA Enterprise Log Manager, è possibile creare un ambiente di raccolta log completamente virtuale. Questo scenario dà per scontato che sia disponibile un numero sufficiente di server, ognuno con un gruppo i almeno quattro processori, per installare ognuno dei server CA Enterprise Log Manager pianificati.

Installare un server CA Enterprise Log Manager per il funzionamento come server di gestione. Durante la configurazione, non inviare registri di eventi a questo server o utilizzare questo server per generare rapporti. Configurando l'ambiente in questo modo verrà mantenuta la velocità di raccolta dei log eventi necessaria per la produzione a livello aziendale.

Generalmente, si procede all'installazione di due server CA Enterprise Log Manager a quattro processori invece che di ciascuno dei server della classe applicazioni normalmente installato quando si utilizzano hardware certificati. (I server della classe applicazioni dispongono di un minimo di otto processori.)

Il processo di creazione di un ambiente virtuale mediante applicazione virtuale include le seguenti procedure:

1. Download del pacchetto dell'applicazione virtuale.
2. Installazione di un server virtuale CA Enterprise Log Manager per funzionalità di gestione.
3. Installazione di due o più server applicazioni per la raccolta e le operazioni di rapporto.
4. Configurazione dei server applicazioni virtuali come descritto nella sezione relativa all'installazione del server CA Enterprise Log Manager.

Importante: Se si desidera eseguire il provisioning di un server CA Enterprise Log Manager mediante applicazione virtuale, il nome dell'istanza applicazione del server CA Enterprise Log Manager primario deve essere CAELM.

Download del pacchetto dell'applicazione virtuale

L'immagine di distribuzione per l'applicazione virtuale CA Enterprise Log Manager è disponibile sul sito del Supporto in linea dal collegamento Download. I file da scaricare sono cinque:

- Il file manifesto
- Il file .ovf
- Tre file di disco virtuale

Formati di recapito OVF

Installazione manuale di un server CA Enterprise Log Manager

Se si installa l'applicazione virtuale manualmente, eseguire le operazioni riportate a continuazione:

1. Distribuire un modello OVF.
2. Definire le impostazioni per la paravirtualizzazione e le risorse.
3. Attivare il server CA Enterprise Log Manager di cui è stato eseguito il provisioning.

Distribuire un modello OVF

È possibile specificare le proprietà dell'applicazione virtuale in un modello OVF. VMware utilizza questo modello per eseguire il provisioning di un server CA Enterprise Log Manager. Utilizzare il client VMware vSphere per eseguire la distribuzione del modello OVF.

Nota: le catture di schermata riportate nelle procedure seguenti contengono dati di esempio. Le catture di schermata riportate fanno riferimento al client VMware vSphere 4.0.0. Si raccomanda di specificare dati consoni al proprio ambiente.

Per distribuire un modello OVF:

1. Fare clic su Start, Programmi, VMware vSphere Client sul computer su cui è installato il client VMware vSphere.

   Viene visualizzata la finestra di dialogo del client VMware vSphere.

2. Nel campo relativo all'indirizzo IP/nome host, immettere l'indirizzo IP o il nome host del server VMware vSphere a cui si desidera effettuare la connessione.

3. Immettere le credenziali di accesso nei campi Nome utente e Password.

4. Fare clic su Logon (Accedi).

   Viene visualizzata la finestra dell'applicazione.

5. Selezionare la posizione in cui si desidera eseguire il provisioning del server CA Enterprise Log Manager sotto un centro dati del riquadro sinistro.

6. Fare clic su File, quindi sull'opzione di distribuzione del modello OVF.

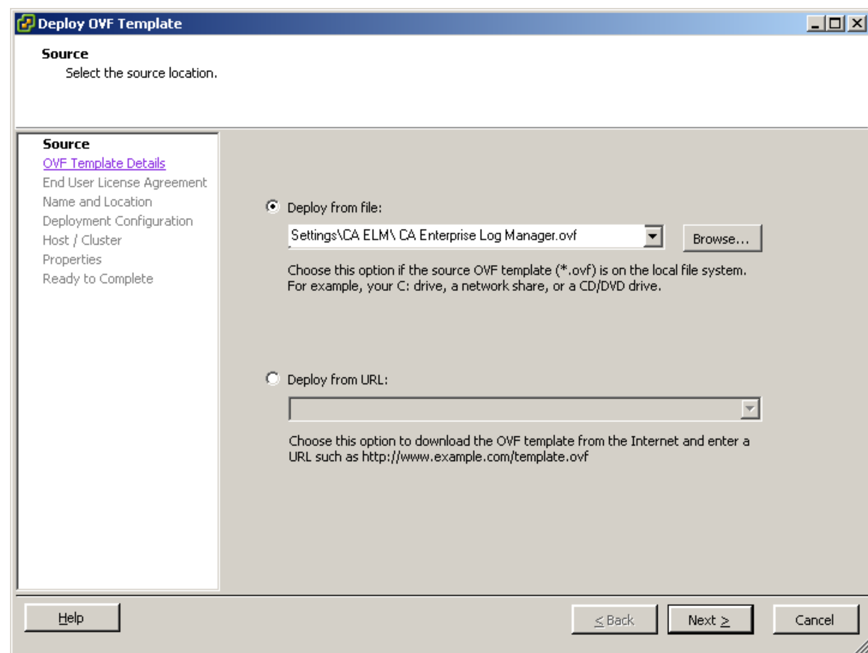
   Viene visualizzata la finestra di distribuzione del modello OVF. Per impostazione predefinita, la finestra di distribuzione del modello OVF visualizza la pagina di origine. Immettere la posizione del modello OVF in questa pagina.

   Nota: le pagine visualizzate nella finestra di distribuzione del modello OVF variano in base alla versione e alle impostazioni del client VMware vSphere in uso. Per ulteriori informazioni sulla distribuzione di un modello OVF, visitare il sito www.vmware.com.

7. Scegliere l'opzione Deploy from file (Distribuisci da file) e fare clic su Sfoglia per selezionare la posizione del modello OVF.

8. Raggiungere la posizione del modello OVF dalla finestra di dialogo Open (Apri), selezionare il modello OVF, quindi fare clic su Apri.

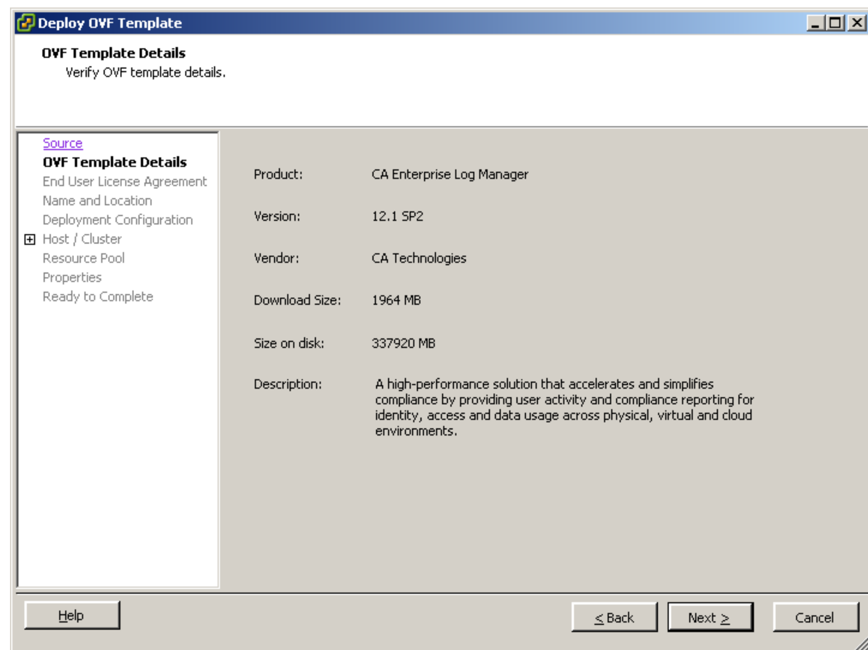
   Il percorso della posizione del modello OVF viene visualizzato nel campo Deploy from file.



9. Fare clic su Avanti.

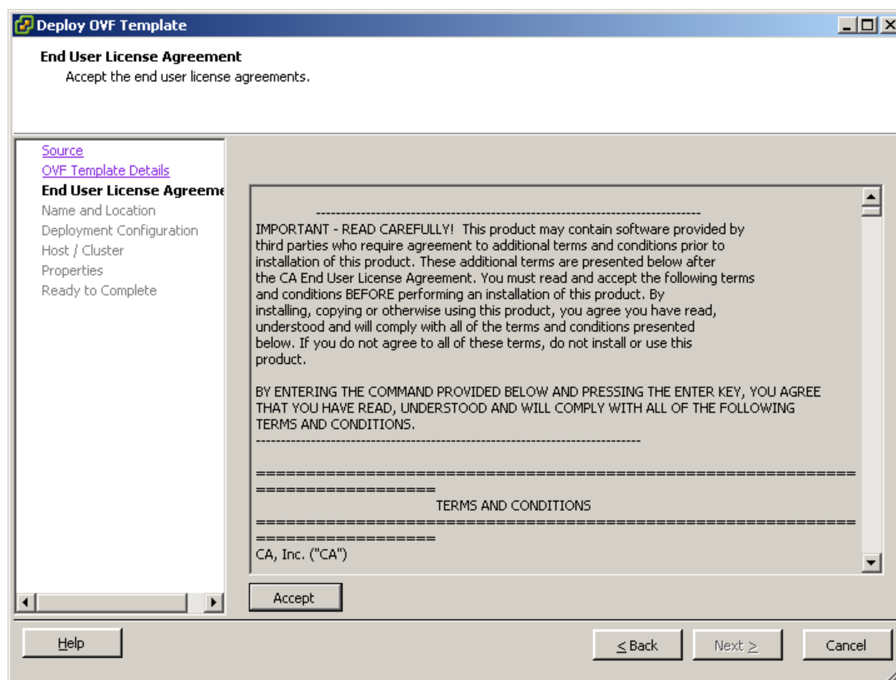
   Viene visualizzata la pagina dei dettagli del modello OVF. La pagina consente di visualizzare i dettagli archiviati nel modello OVF, quali le dimensioni di download, lo spazio su disco disponibile e il nome del fornitore.

10. Verificare di disporre di un minimo di 350 GB di spazio su disco sul server VMware, quindi fare clic su Avanti.



Viene visualizzata la pagina del contratto di licenza per l'utente finale. In questa pagina viene visualizzato il contratto di licenza per i prodotti di terze parti. Sarà necessario accettare il contratto di licenza per poter procedere all'installazione di CA Enterprise Log Manager.

11. Leggere il testo del contratto.

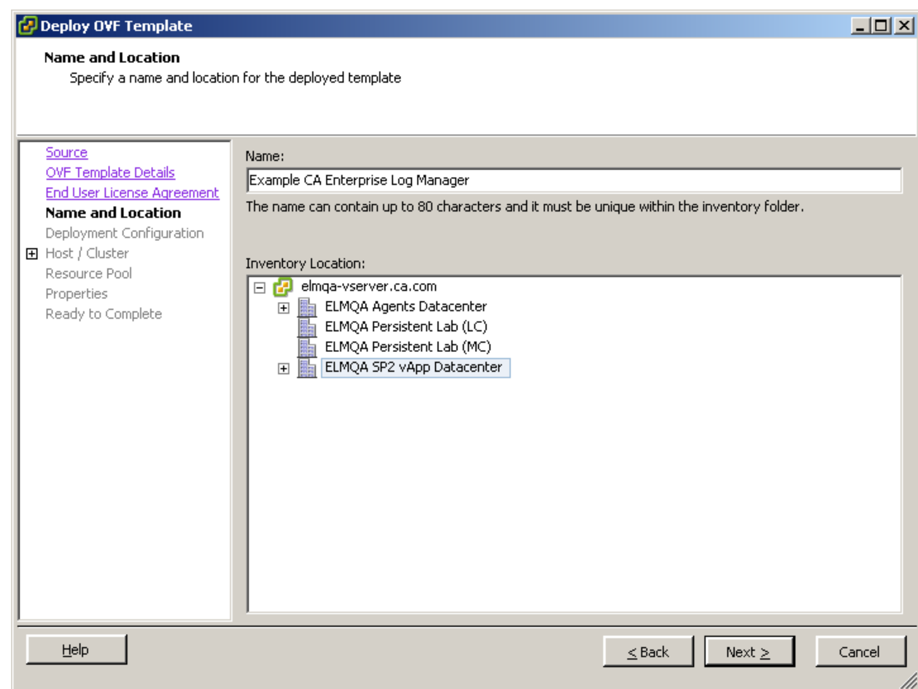


12. Accettare i termini del contratto, quindi fare clic su Avanti.

    Verrà visualizzata la pagina relativa al nome e alla posizione. In questa pagina sarà possibile indicare un nome per identificare il server CA Enterprise Log Manager e specificare il centro dati in cui si desidera eseguire il provisioning del server CA Enterprise Log Manager.

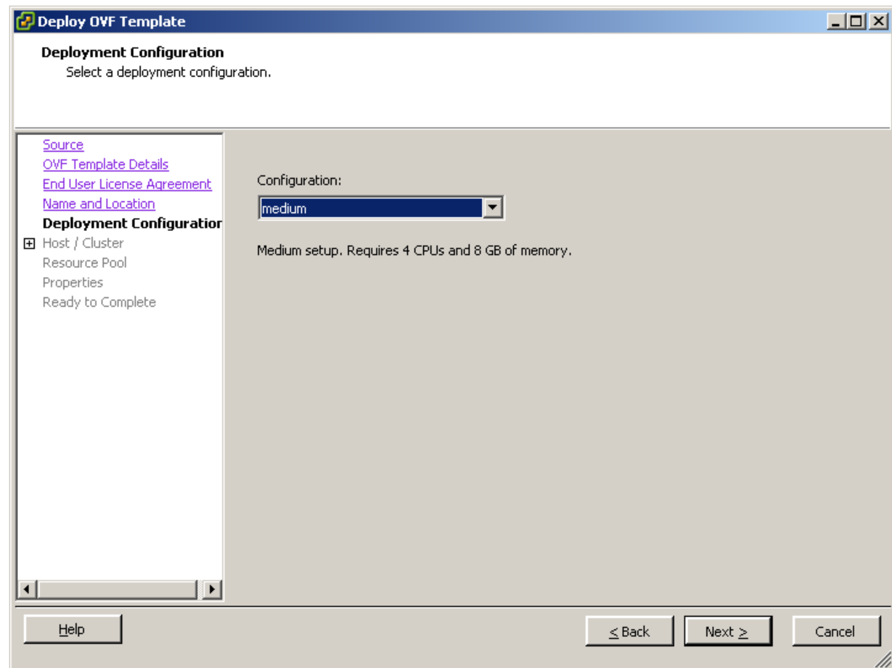
13. Immettere il nome del server CA Enterprise Log Manager nel campo Nome, selezionare il centro dati da Inventory Location (Posizione inventario), quindi fare clic su Avanti.

    Nota: per impostazione predefinita, il nome specificato nel modello OVF viene visualizzato nel campo Nome.



Viene visualizzata la pagina di configurazione della distribuzione. La pagina della configurazione di distribuzione consente di specificare la modalità di configurazione del serverCA Enterprise Log Manager di cui si desidera effettuare il provisioning.

14. Dal menu a discesa Configurazione, selezionare Medium (Media) o Large (Estesa), quindi fare clic su Avanti.

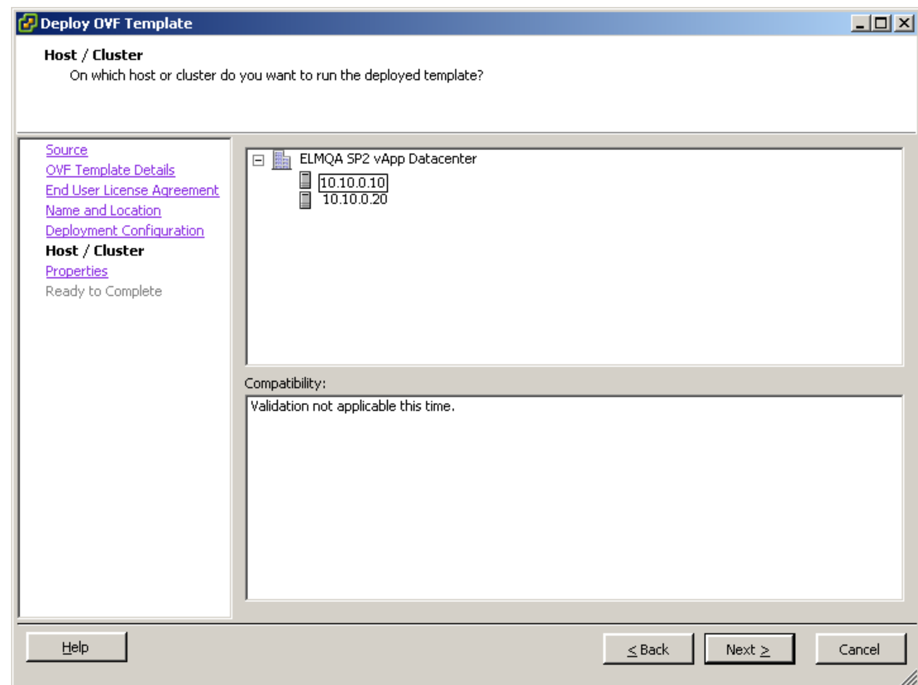


Se si seleziona Media, VMware indica quattro CPU con 8 GB di RAM ciascuna. Se si seleziona Estesa, VMware indica otto CPU con 8 GB di RAM ciascuna.

Nota: si consiglia di utilizzare una configurazione di distribuzione media per effettuare il provisioning di un server di raccolta e una configurazione di distribuzione estesa per effettuare il provisioning di un server di gestione o di rapporto.

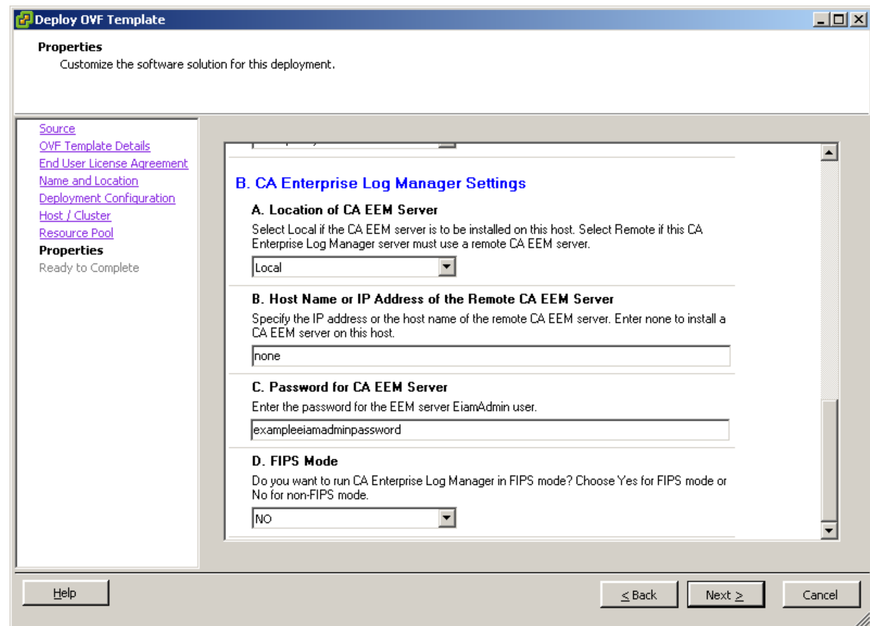
Si aprirà la pagina Host/Cluster. Questa pagina viene visualizzata solo se non è stato selezionato il pool di risorse prima di avviare l'importazione del modello OVF. La pagina Host/Cluster visualizza il centro dati selezionato e i cluster disponibili. È necessario specificare la posizione del cluster nel centro dati in cui si desidera eseguire il provisioning del server CA Enterprise Log Manager.

15. Selezionare un cluster nel centro dati, quindi fare clic su Avanti.



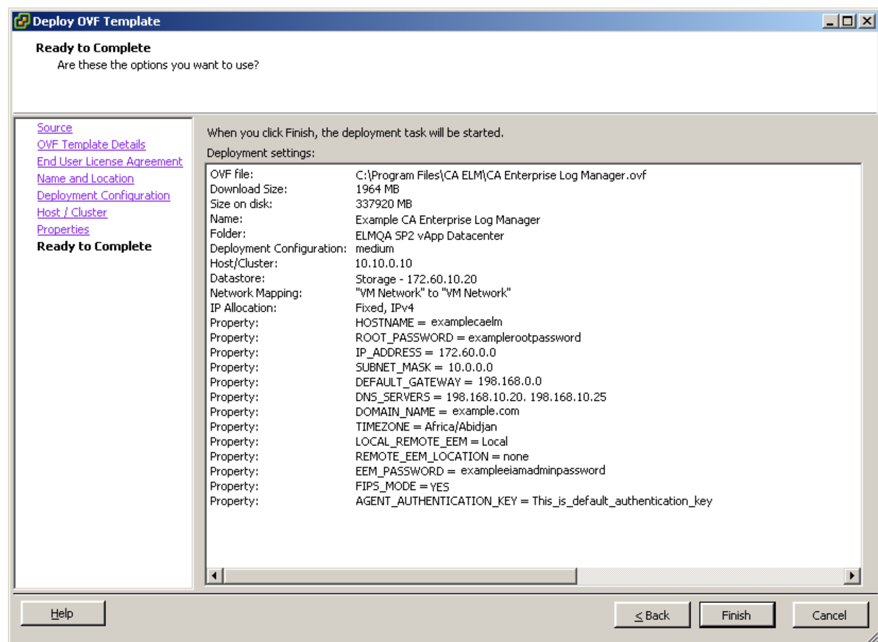
Viene visualizzata la pagina delle proprietà. Questa pagina contiene le impostazioni dell'host e di CA Enterprise Log Manager.

16. Immettere i valori per ciascun campo utilizzando le informazioni raccolte nel foglio di lavoro di installazione, quindi fare clic su Avanti.



Viene visualizzata la pagina Ready to Complete (Pronto per il completamento). La pagina visualizza un riepilogo delle informazioni immesse nelle pagine precedenti.

17. Verificare le informazioni immesse, quindi fare clic su Fine.



Viene visualizzato il messaggio Opening VI target (Apertura destinazione VI in corso...) Viene visualizzato lo stato di distribuzione dell'applicazione virtuale. Se l'installazione viene completata correttamente, l'applicazione virtuale viene visualizzata nel centro dati selezionato nel riquadro sinistro.

18. (Facoltativo) Se si desidera modificare le informazioni immesse, eseguire le seguenti operazioni:

    a. Nella finestra relativa alla distribuzione del modello OVF, fare clic ripetutamente su Indietro fino a raggiungere la pagina da modificare.

    b. Apportare le modifiche necessarie.

    c. Quindi, fare clic ripetutamente su Avanti fino a raggiungere la pagina Ready to Complete (Pronto per il completamento).

Definizione delle impostazioni per la paravirtualizzazione e le risorse

Dopo aver importato il modello OVF, è necessario definire manualmente le impostazioni della paravirtualizzazione e delle risorse per migliorare le prestazioni del server CA Enterprise Log Manager di cui è stato eseguito il provisioning.

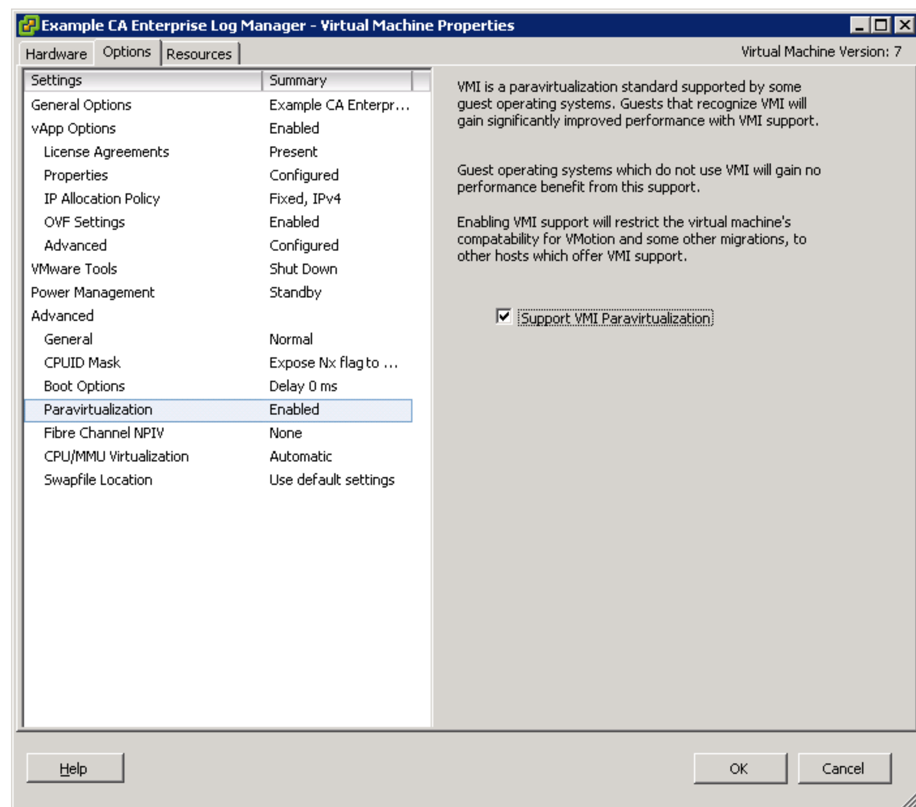
Per definire le impostazioni della paravirtualizzazione e delle risorse:

1. Fare clic con il pulsante destro del mouse sulla nuova applicazione virtuale di CA Enterprise Log Manager nel riquadro sinistro, quindi sull'opzione di modifica impostazioni.

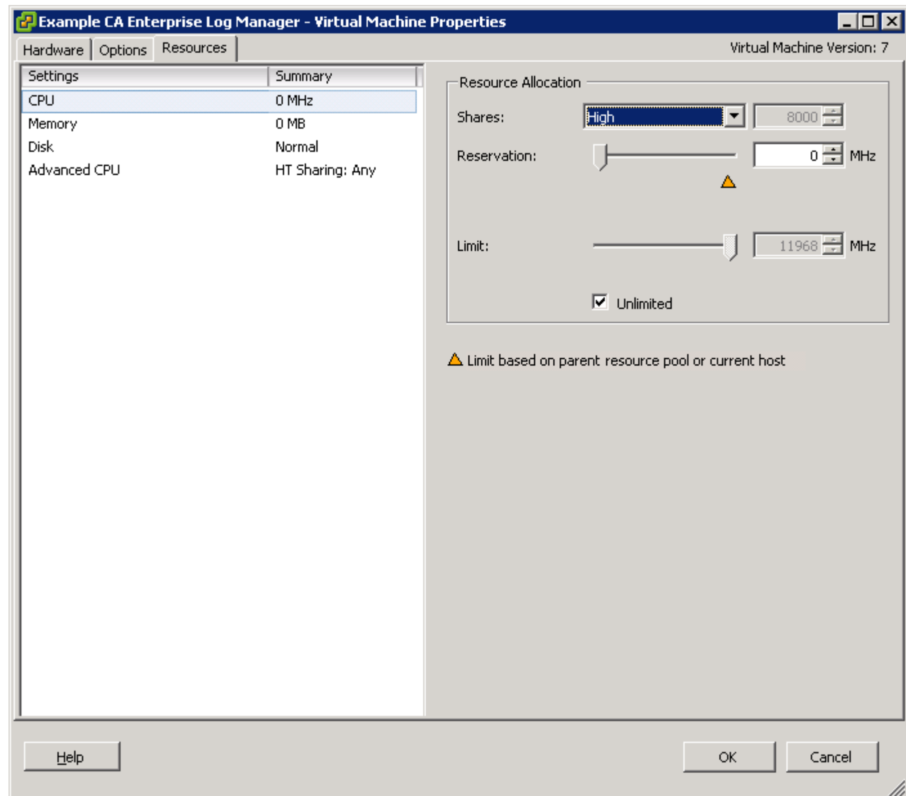
   Viene visualizzata la finestra <*CA Enterprise Log Manager Virtual Appliance name*> - Virtual Machine Properties (Proprietà del computer virtuale <CA Enterprise Log Manager Virtual Appliance name>)

2. Fare clic sulla scheda Opzioni.

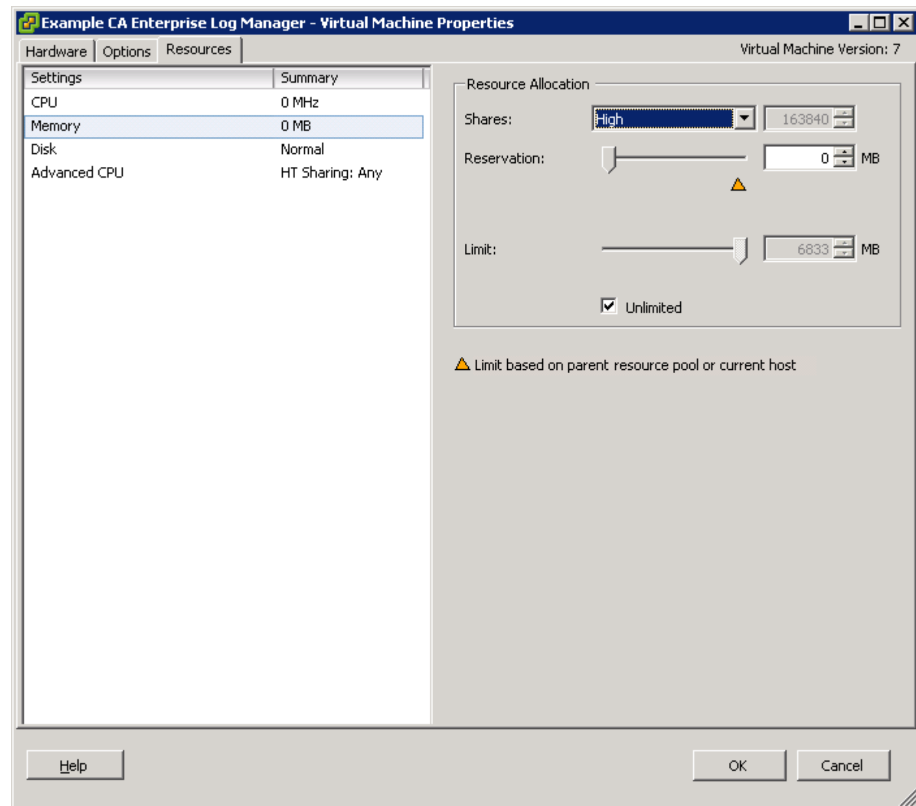
3. Selezionare l'impostazione di paravirtualizzazione nel riquadro sinistro quindi l'opzione per il supporto della paravirtualizzazione VMI nel riquadro destro.



4. Fare clic sulla scheda Risorse.
5. Selezionare l'opzione CPU nella colonna Impostazioni, quindi selezionare High (Alta) dal menu a discesa Shares (Condivisioni) nella sezione Resource allocation (Allocazione risorse).



6. Selezionare l'opzione Memory (Memoria) nella colonna Impostazioni, quindi selezionare High (Alta) dal menu a discesa Shares (Condivisioni) nella sezione Resource allocation (Allocazione risorse).



7. Fare clic su OK.

8. **Nota**: per ulteriori informazioni sulla paravirtualizzazione, si rimanda al sito www.vmware.com.

Attivare il server CA Enterprise Log Manager di cui è stato eseguito il provisioning.

Il server CA Enterprise Log Manager deve essere attivato per poter dare inizio all'esecuzione.

Per attivare un server CA Enterprise Log Manager:

1. Selezionare il nuovo server CA Enterprise Log Manager nel riquadro sinistro della finestra dell'applicazione VMware.
2. Fare clic sull'opzione di avvio in Basic Tasks (Attività di base) della scheda Getting Started (Introduzione) del riquadro destro.

   Il server CA Enterprise Log Manager verrà attivato.

Nota: verificare che un server primario CA Enterprise Log Manager sia in esecuzione prima di attivare un server secondario CA Enterprise Log Manager.

Installazione invisibile di un server CA Enterprise Log Manager

Quando si procede all'installazione dell'applicazione virtuale in modalità invisibile all'utente, è necessario eseguire le seguenti operazioni:

1. Richiamare lo strumento OVF.
2. Definire le impostazioni per la paravirtualizzazione e le risorse.
3. Attivare il server CA Enterprise Log Manager di cui è stato eseguito il provisioning.

La tabella seguente descrive i parametri utilizzati per eseguire la distribuzione di CA Enterprise Log Manager mediante lo strumento OVF. È necessario specificare tali parametri come argomenti della riga di comando.

Informazioni necessarie	Valore	Commenti
Impostazioni specifiche dell'host		

Informazioni necessarie	Valore	Commenti
HOSTNAME	*Nome host del server CA Enterprise Log Manager* Ad esempio: CA-ELM1	Specificare il nome host del server utilizzando solo i caratteri supportati per gli host. Gli standard industriali consigliano l'utilizzo dei caratteri A-Z (senza distinzione di maiuscole), 0-9 ed i trattini, dove il primo carattere corrisponde ad una lettera e l'ultimo ad un carattere alfanumerico. Non utilizzare il trattino basso all'interno del nome host né aggiungere un nome di dominio all'host. **Nota:**: il nome host non può superare i 15 caratteri.
ROOT_PASSWORD	*nuova password principale*	Creare e confermare una nuova password per il server.
IP_ADDRESS	*Indirizzo IPv4 rilevante*	Inserire un indirizzo IP valido per il server.
SUBNET_MASK	*Indirizzo IP rilevante*	Inserire una subnet mask valida da utilizzare con il server.
DEFAULT_GATEWAY	*Indirizzo IP rilevante*	Inserire una subnet mask ed un gate predefinito da utilizzare con il server.
DNS_SERVERS	*Indirizzi IPv4 corrispondenti*	Immettere uno o più indirizzi IP di server DNS utilizzati nella rete. elenco separato da virgole senza spazi tra le voci. Se i server DNS utilizzano indirizzi IPv6, immettere questi indirizzi in quel formato.
DOMAIN_NAME	*il nome del dominio*	Inserire il nome di dominio completo del server, ad esempio mycompany.com. **Nota:** per abilitare la risoluzione del nome host nell'indirizzo IP è necessario registrare il nome del dominio sul server DNS di rete.
acceptAllEulas	Accetta	Accettare il contratto di licenza di CA per procedere con il provisioning del server CA Enterprise Log Manager.
deploymentOption	medium (media) o large (estesa).	Se si seleziona Media, VMware indica quattro CPU con 8 GB di RAM ciascuna. Se si seleziona Estesa, VMware indica otto CPU con 8 GB di RAM ciascuna.

Informazioni necessarie	Valore	Commenti
TIMEZONE	*fuso orario desiderato*	Selezionare il fuso orario del server.
Impostazioni specifiche dell'applicazione		
LOCAL_REMOTE_EEM	Locale: per il primo server installato (server di gestione) Remoto: per ogni server aggiuntivo	Indicare se si desidera utilizzare un server CA EEM locale o remoto. Per un server di gestione CA Enterprise Log Manager, scegliere il server remoto. L'installazione richiede di creare una password per l'account utente EiamAdmin predefinito. Per ogni server aggiuntivo, scegliere Remoto. L'installazione richiede il nome del server di gestione. Indipendentemente dal tipo di server scelto (locale o remoto), è necessario utilizzare l'ID e la password dell'account EiamAdmin per il primo accesso al server CA Enterprise Log Manager.
REMOTE_EEM_LOCATION	*Nome host o indirizzo IP*	Specificare questo valore solo se si seleziona l'opzione server remota. Immettere l'indirizzo IP o il nome host del server di gestione CA Enterprise Log Manager installato per primo. Il nome host deve essere registrato con il server DNS. Se si desidera utilizzare un server CA EEM locale, il valore predefinito è **Nessuno**.

Informazioni necessarie	Valore	Commenti
EEM_PASSWORD	*Password account EiamAdmin*	Registrare la password per l'account amministratore predefinito, EiamAdmin. L'accesso iniziale al server CA Enterprise Log Manager richiede queste credenziali dell'account. Se si installa il server di gestione, creare e confermare qui la nuova password EiamAdmin. Annotare questa password, in quanto verrà utilizzata nuovamente durante le installazioni degli altri server e agenti CA Enterprise Log Manager. **Nota**: la password immessa sarà anche la password iniziale dell'account caelmadmin predefinito utilizzato per accedere direttamente al server CA Enterprise Log Manager attraverso ssh. È possibile creare ulteriori account di amministratore per accedere alle funzioni CA EEM dopo l'installazione, se lo si desidera.
FIPS_MODE	Sì o No	Specifica se l'applicazione virtuale deve essere eseguita in modalità FIPS o non-FIPS. Se si sceglie di utilizzare un server CA EEM locale, è possibile selezionare qualsiasi modalità. Se si sceglie di utilizzare un server CA EEM remoto, è necessario selezionare la modalità utilizzata dal server remoto CA EEM.

Ulteriori informazioni

Aggiunta di server virtuali all'ambiente (a pagina 325)
Creazione di un ambiente completamente virtuale (a pagina 348)
Distribuzione rapida di server virtuali (a pagina 373)

Richiamare lo strumento OVF dalla riga di comando

Nota: è necessario installare lo strumento OVF 1.0.0.0 prima di eseguire l'installazione invisibile all'utente. Per ulteriori informazioni sullo strumento OVF, consultare la *Guida per l'utente dello strumento OVF* oppure visitare il sito www.vmware.com.

Per richiamare lo strumento OVF, è necessario passare i parametri di configurazione come argomenti della riga di comando.

Nota: si consiglia di utilizzare una configurazione di distribuzione media per effettuare il provisioning di un server di raccolta e una configurazione di distribuzione estesa per effettuare il provisioning di un server di rapporto. È consigliabile anche utilizzare il metodo di distribuzione thick come descritto nella documentazione VMware.

Per richiamare lo strumento OVF dalla riga di comando:

1. Aprire il prompt dei comandi sul computer in cui è installato VMware vSphere Client.
2. Per richiamare lo strumento OVF, eseguire il seguente comando:

   ```
   ovftool -dm=thick --acceptAllEulas --name=value --deploymentOption=value --
   prop:ROOT_PASSWORD=value --prop:LOCAL_REMOTE_EEM=value --
   prop:REMOTE_EEM_LOCATION=value --prop:EEM_PASSWORD=value --
   prop:FIPS_MODE=value --prop:IP_ADDRESS=value --prop:SUBNET_MASK=value --
   prop:HOSTNAME=value --prop:DEFAULT_GATEWAY=value --prop:DNS_SERVERS=value --
   prop:DOMAIN_NAME=value --prop:TIMEZONE=value <OVF_Name.ovf>
   vi://username:password@hostname_of_VMware_vSphere_Client/Datacenter/host/host
   name
   ```

   Viene visualizzato il messaggio Opening VI target (Apertura destinazione VI in corso...) Viene visualizzato lo stato di distribuzione del server CA Enterprise Log Manager. Se l'installazione viene completata correttamente, il server CA Enterprise Log Manager viene visualizzata nel centro dati selezionato nel riquadro sinistro.

   Note: se il valore di una proprietà contiene spazi, racchiudere il valore tra virgolette doppie (""). Ad esempio, se il nome OVF è CA ELM, immettere il valore come "CA ELM.ovf". Per ulteriori informazioni sullo strumento OVF, consultare la *Guida per l'utente dello strumento OVF*.

Esempio

```
ovftool -dm=thick --acceptAllEulas --name="example_server" --
deploymentOption=medium --prop:ROOT_PASSWORD="example_password" --
prop:LOCAL_REMOTE_EEM=Local --prop:REMOTE_EEM_LOCATION=none --
prop:EEM_PASSWORD=calmr12 --prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172,168.0,0 --
prop:SUBNET_MASK=10,0.0,0 --prop:HOSTNAME="example_server1" --
prop:DEFAULT_GATEWAY=198,168.0,0 --prop:DNS_SERVERS=198,168.10,20,198,168.10,25 -
-prop:DOMAIN_NAME=example.com --prop:TIMEZONE=Asia/Kolkata "C:\Program Files\CA
ELM\CA Enterprise Log Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0,10.0
"
```

Definizione delle impostazioni per la paravirtualizzazione e le risorse

Dopo aver importato il modello OVF, è necessario definire manualmente le impostazioni della paravirtualizzazione e delle risorse per migliorare le prestazioni del server CA Enterprise Log Manager di cui è stato eseguito il provisioning.

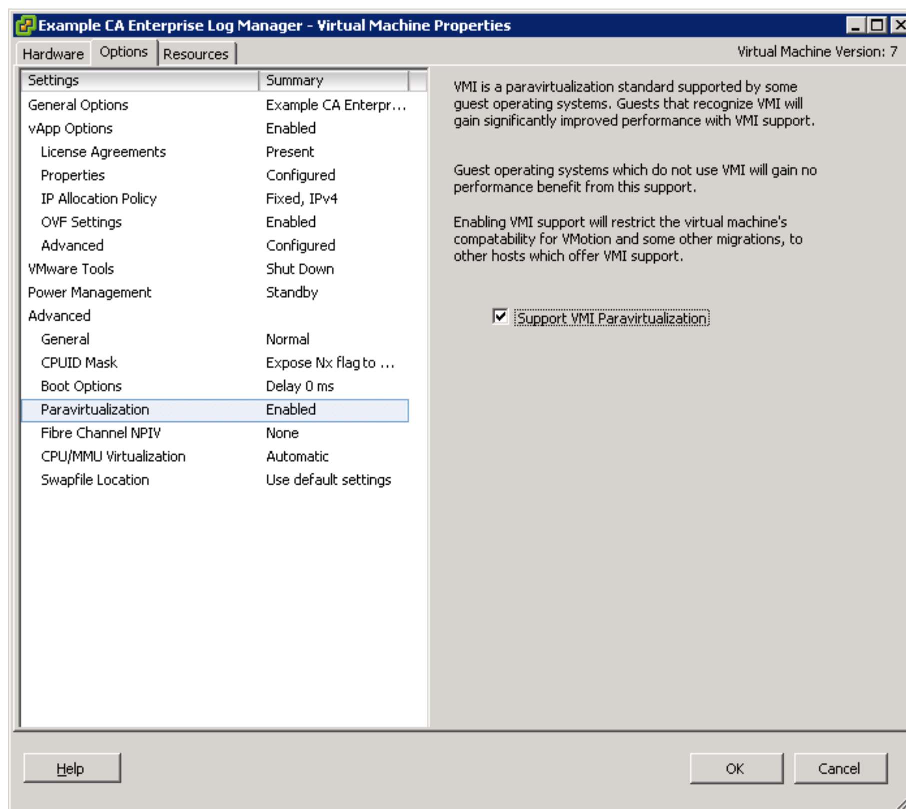
Per definire le impostazioni della paravirtualizzazione e delle risorse:

1. Fare clic con il pulsante destro del mouse sulla nuova applicazione virtuale di CA Enterprise Log Manager nel riquadro sinistro, quindi sull'opzione di modifica impostazioni.

   Viene visualizzata la finestra <*CA Enterprise Log Manager Virtual Appliance name*> - Virtual Machine Properties (Proprietà del computer virtuale <CA Enterprise Log Manager Virtual Appliance name>)

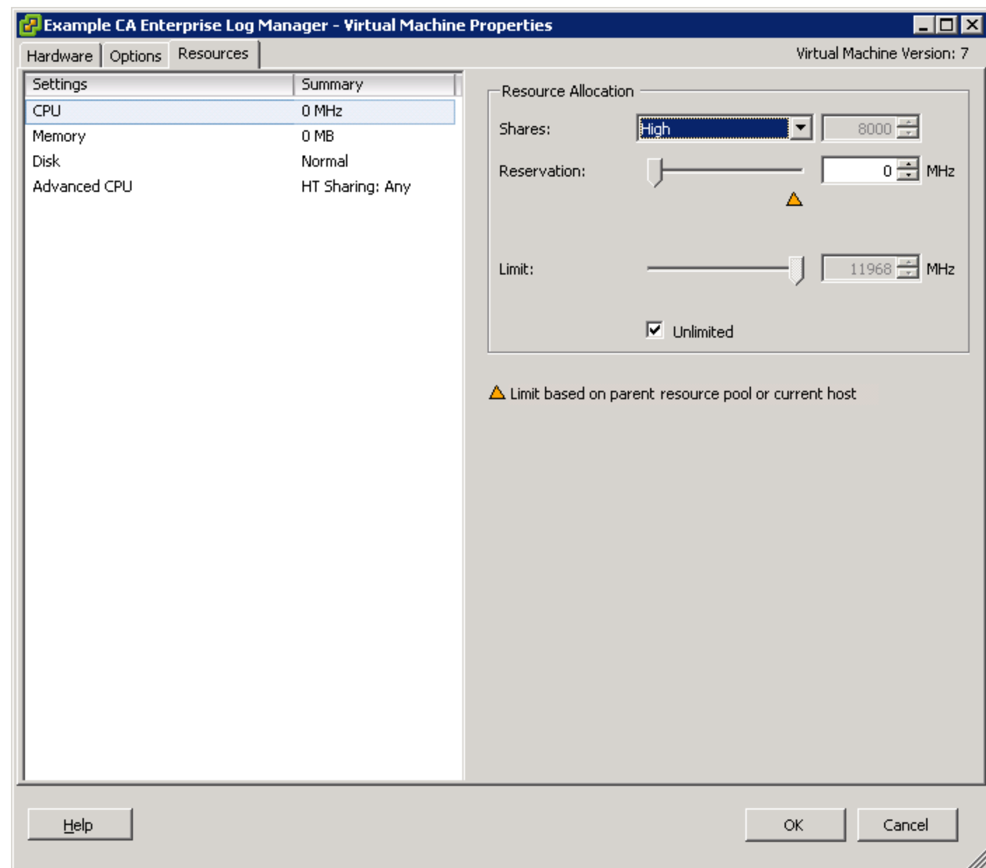
2. Fare clic sulla scheda Opzioni.

3. Selezionare l'impostazione di paravirtualizzazione nel riquadro sinistro quindi l'opzione per il supporto della paravirtualizzazione VMI nel riquadro destro.

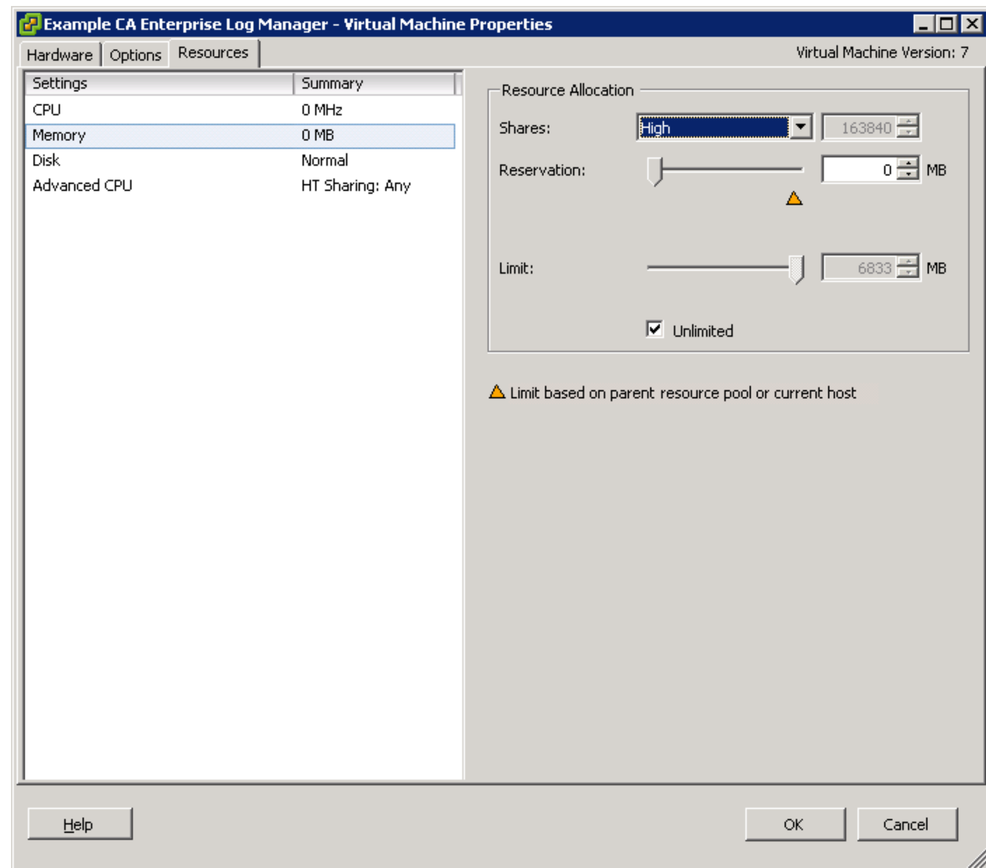


4. Fare clic sulla scheda Risorse.

5. Selezionare l'opzione CPU nella colonna Impostazioni, quindi selezionare High (Alta) dal menu a discesa Shares (Condivisioni) nella sezione Resource allocation (Allocazione risorse).



6. Selezionare l'opzione Memory (Memoria) nella colonna Impostazioni, quindi selezionare High (Alta) dal menu a discesa Shares (Condivisioni) nella sezione Resource allocation (Allocazione risorse).



7. Fare clic su OK.

8. **Nota**: per ulteriori informazioni sulla paravirtualizzazione, si rimanda al sito www.vmware.com.

Attivare il server CA Enterprise Log Manager di cui è stato eseguito il provisioning.

Il server CA Enterprise Log Manager deve essere attivato per poter dare inizio all'esecuzione.

Per attivare un server CA Enterprise Log Manager:

1. Selezionare il nuovo server CA Enterprise Log Manager nel riquadro sinistro della finestra dell'applicazione VMware.
2. Fare clic sull'opzione di avvio in Basic Tasks (Attività di base) della scheda Getting Started (Introduzione) del riquadro destro.

   Il server CA Enterprise Log Manager verrà attivato.

Nota: verificare che un server primario CA Enterprise Log Manager sia in esecuzione prima di attivare un server secondario CA Enterprise Log Manager.

Verifica dell'installazione di un server virtuale CA Enterprise Log Manager

Quando si attiva il server CA Enterprise Log Manager di cui è stato eseguito il provisioning, nella scheda della console della finestra del client VMware vSphere viene visualizzato un URL di accesso a CA Enterprise Log Manager. Utilizzare l'URL e le credenziali di accesso predefinito riportate di seguito per accedere a CA Enterprise Log Manager:

Nome utente predefinito: EiamAdmin

Password predefinita: la password immessa durante la procedura di installazione del server CA Enterprise Log Manager

Ulteriori informazioni

Aggiunta di server virtuali all'ambiente (a pagina 325)
Creazione di un ambiente completamente virtuale (a pagina 348)
Distribuzione rapida di server virtuali (a pagina 373)

Distribuzione rapida di server virtuali

Il processo seguito per la distribuzione rapida di un server CA Enterprise Log Manager virtuale per la raccolta include le seguenti procedure:

1. Download del pacchetto dell'applicazione virtuale CA Enterprise Log Manager.
2. Installazione di un server CA Enterprise Log Manager in modalità invisibile all'utente
3. Configurazione dei server applicazioni virtuali come descritto nella sezione relativa all'installazione del server CA Enterprise Log Manager.

Importante: Se si desidera eseguire il provisioning di un server CA Enterprise Log Manager mediante applicazione virtuale, il nome dell'istanza applicazione del server CA Enterprise Log Manager primario deve essere CAELM.

Download del pacchetto dell'applicazione virtuale

L'immagine di distribuzione per l'applicazione virtuale CA Enterprise Log Manager è disponibile sul sito del Supporto in linea dal collegamento Download. I file da scaricare sono cinque:

- Il file manifesto
- Il file .ovf
- Tre file di disco virtuale

Installazione invisibile di un server CA Enterprise Log Manager

Quando si procede all'installazione dell'applicazione virtuale in modalità invisibile all'utente, è necessario eseguire le seguenti operazioni:

1. Richiamare lo strumento OVF.
2. Definire le impostazioni per la paravirtualizzazione e le risorse.
3. Attivare il server CA Enterprise Log Manager di cui è stato eseguito il provisioning.

La tabella seguente descrive i parametri utilizzati per eseguire la distribuzione di CA Enterprise Log Manager mediante lo strumento OVF. È necessario specificare tali parametri come argomenti della riga di comando.

Informazioni necessarie	Valore	Commenti
Impostazioni specifiche dell'host		

Informazioni necessarie	Valore	Commenti
HOSTNAME	*Nome host del server CA Enterprise Log Manager* Ad esempio: CA-ELM1	Specificare il nome host del server utilizzando solo i caratteri supportati per gli host. Gli standard industriali consigliano l'utilizzo dei caratteri A-Z (senza distinzione di maiuscole), 0-9 ed i trattini, dove il primo carattere corrisponde ad una lettera e l'ultimo ad un carattere alfanumerico. Non utilizzare il trattino basso all'interno del nome host né aggiungere un nome di dominio all'host. **Nota:**: il nome host non può superare i 15 caratteri.
ROOT_PASSWORD	*nuova password principale*	Creare e confermare una nuova password per il server.
IP_ADDRESS	*Indirizzo IPv4 rilevante*	Inserire un indirizzo IP valido per il server.
SUBNET_MASK	*Indirizzo IP rilevante*	Inserire una subnet mask valida da utilizzare con il server.
DEFAULT_GATEWAY	*Indirizzo IP rilevante*	Inserire una subnet mask ed un gate predefinito da utilizzare con il server.
DNS_SERVERS	*Indirizzi IPv4 corrispondenti*	Immettere uno o più indirizzi IP di server DNS utilizzati nella rete. elenco separato da virgole senza spazi tra le voci. Se i server DNS utilizzano indirizzi IPv6, immettere questi indirizzi in quel formato.
DOMAIN_NAME	*il nome del dominio*	Inserire il nome di dominio completo del server, ad esempio mycompany.com. **Nota:** per abilitare la risoluzione del nome host nell'indirizzo IP è necessario registrare il nome del dominio sul server DNS di rete.
acceptAllEulas	Accetta	Accettare il contratto di licenza di CA per procedere con il provisioning del server CA Enterprise Log Manager.
deploymentOption	medium (media) o large (estesa).	Se si seleziona Media, VMware indica quattro CPU con 8 GB di RAM ciascuna. Se si seleziona Estesa, VMware indica otto CPU con 8 GB di RAM ciascuna.

Informazioni necessarie	Valore	Commenti
TIMEZONE	*fuso orario desiderato*	Selezionare il fuso orario del server.
Impostazioni specifiche dell'applicazione		
LOCAL_REMOTE_EEM	Locale: per il primo server installato (server di gestione) Remoto: per ogni server aggiuntivo	Indicare se si desidera utilizzare un server CA EEM locale o remoto. Per un server di gestione CA Enterprise Log Manager, scegliere il server remoto. L'installazione richiede di creare una password per l'account utente EiamAdmin predefinito. Per ogni server aggiuntivo, scegliere Remoto. L'installazione richiede il nome del server di gestione. Indipendentemente dal tipo di server scelto (locale o remoto), è necessario utilizzare l'ID e la password dell'account EiamAdmin per il primo accesso al server CA Enterprise Log Manager.
REMOTE_EEM_LOCATION	*Nome host o indirizzo IP*	Specificare questo valore solo se si seleziona l'opzione server remota. Immettere l'indirizzo IP o il nome host del server di gestione CA Enterprise Log Manager installato per primo. Il nome host deve essere registrato con il server DNS. Se si desidera utilizzare un server CA EEM locale, il valore predefinito è **Nessuno**.

Informazioni necessarie	Valore	Commenti
EEM_PASSWORD	*Password account EiamAdmin*	Registrare la password per l'account amministratore predefinito, EiamAdmin. L'accesso iniziale al server CA Enterprise Log Manager richiede queste credenziali dell'account. Se si installa il server di gestione, creare e confermare qui la nuova password EiamAdmin. Annotare questa password, in quanto verrà utilizzata nuovamente durante le installazioni degli altri server e agenti CA Enterprise Log Manager. **Nota**: la password immessa sarà anche la password iniziale dell'account caelmadmin predefinito utilizzato per accedere direttamente al server CA Enterprise Log Manager attraverso ssh. È possibile creare ulteriori account di amministratore per accedere alle funzioni CA EEM dopo l'installazione, se lo si desidera.
FIPS_MODE	Sì o No	Specifica se l'applicazione virtuale deve essere eseguita in modalità FIPS o non-FIPS. Se si sceglie di utilizzare un server CA EEM locale, è possibile selezionare qualsiasi modalità. Se si sceglie di utilizzare un server CA EEM remoto, è necessario selezionare la modalità utilizzata dal server remoto CA EEM.

Ulteriori informazioni

Aggiunta di server virtuali all'ambiente (a pagina 325)
Creazione di un ambiente completamente virtuale (a pagina 348)
Distribuzione rapida di server virtuali (a pagina 373)

Richiamare lo strumento OVF tramite script

Nota: è necessario installare lo strumento OVF 4.0.0 prima di eseguire l'installazione invisibile all'utente. Per ulteriori informazioni sullo strumento OVF, consultare la guida *VMware's OVF Tool User Guide* oppure visitare il sito www.vmware.com.

È possibile installare più server CA Enterprise Log Manager simultaneamente, creando ed eseguendo script contenenti il comando per richiamare lo strumento OVF. È possibile utilizzare qualsiasi linguaggio di scripting per la creazione di script.

Per richiamare lo strumento OVF tramite script:

1. Creare uno script per richiamare lo strumento OVF.
2. Aprire il prompt dei comandi sul computer in cui è installato VMware vSphere Client.
3. Accedere al percorso in cui è stato memorizzato lo script.
4. Eseguire lo script.

   Viene visualizzato il messaggio Opening VI target (Apertura destinazione VI in corso...) Viene visualizzato lo stato di distribuzione di ciascun server CA Enterprise Log Manager. Se l'installazione viene completata correttamente, il server CA Enterprise Log Manager viene visualizzato nel centro dati selezionato nel riquadro sinistro.

Esempio 1: Script batch per la creazione di un server primario e di un server secondario CA Enterprise Log Manager

```
Server primario CA Enterprise Log Manager REM
ovftool -dm=thin --acceptAllEulas --name="example_primaryserver" --
deploymentOption=medium --prop:ROOT_PASSWORD="example_password" --
prop:LOCAL_REMOTE_EEM=Local --prop:REMOTE_EEM_LOCATION=none --
prop:EEM_PASSWORD=calmr12 --prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172,162.0,0 --
prop:SUBNET_MASK=10,0.0,0 --prop:HOSTNAME="example_primary_server" --
prop:DEFAULT_GATEWAY=198,168.0,0 --prop:DNS_SERVERS=198,168.10,20,198,168.10,25 -
-prop:DOMAIN_NAME=example.com --prop:TIMEZONE=Asia/Kolkata "C:\Program Files\CA
ELM\CA Enterprise Log Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0,10.0
"

Server secondario CA Enterprise Log Manager REM
```

```
ovftool -dm=thin --acceptAllEulas --name="example_secondaryserver" --
deploymentOption=medium --prop:ROOT_PASSWORD="example_password1" --
prop:LOCAL_REMOTE_EEM="Remote" --prop:REMOTE_EEM_LOCATION="example_primaryserver"
--prop:EEM_PASSWORD="calmr12" --prop:FIPS_MODE="Yes" --
prop:IP_ADDRESS="172,168.10,10" --prop:SUBNET_MASK="10,0.10,10" --
prop:HOSTNAME="example_secondary_server" --prop:DEFAULT_GATEWAY="198,168.10,30" -
-prop:DNS_SERVERS="198,168.20,20,198,168.20,25" --prop:DOMAIN_NAME="example.com"
--prop:TIMEZONE="Asia/Kolkata" "C:\Program Files\CA ELM\CA Enterprise Log
Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0,10.0
"
```

Esempio 2: Script batch per la creazione di un server di gestione e due server di raccolta

```
Server di gestione CA Enterprise Log Manager REM
ovftool -dm=thin --acceptAllEulas --name="example_managementserver" --
deploymentOption=medium --prop:ROOT_PASSWORD="example_password" --
prop:LOCAL_REMOTE_EEM=Local --prop:REMOTE_EEM_LOCATION=none --
prop:EEM_PASSWORD=calmr12 --prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172,168.0,0 --
prop:SUBNET_MASK=10,0.0,0 --prop:HOSTNAME="example_management_server" --
prop:DEFAULT_GATEWAY=198,168.0,0 --prop:DNS_SERVERS=198,168.10,20,198,168.10,25 -
-prop:DOMAIN_NAME=example.com --prop:TIMEZONE=Asia/Kolkata "C:\Program Files\CA
ELM\CA Enterprise Log Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0,10.0
"

Server di raccolta CA Enterprise Log Manager REM 1
ovftool -dm=thin --acceptAllEulas --name="example_collectionserver1" --
deploymentOption=medium --prop:ROOT_PASSWORD="example_password1" --
prop:LOCAL_REMOTE_EEM=Remote --
prop:REMOTE_EEM_LOCATION="example_managementserver" --prop:EEM_PASSWORD=calmr12 -
-prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172,168.10,10 --prop:SUBNET_MASK=10,0.10,10
--prop:HOSTNAME="example_collection_server1" --prop:DEFAULT_GATEWAY=198,168.10,30
--prop:DNS_SERVERS=198,168.20,20,198,168.20,25 --prop:DOMAIN_NAME=example.com --
prop:TIMEZONE=Asia/Kolkata "C:\Program Files\CA ELM\CA Enterprise Log
Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0,10.0
"

Server di raccolta CA Enterprise Log Manager REM 2
```

```
ovftool -dm=thin --acceptAllEulas --name="example_collectionserver2" --
deploymentOption=medium --prop:ROOT_PASSWORD="example_password2" --
prop:LOCAL_REMOTE_EEM=Remote --
prop:REMOTE_EEM_LOCATION="example_managementserver" --prop:EEM_PASSWORD=calmr12 -
-prop:FIPS_MODE=Yes --prop:IP_ADDRESS=172,168.10,30 --prop:SUBNET_MASK=10,0.10,40
--prop:HOSTNAME="example_collection_server2" --prop:DEFAULT_GATEWAY=198,168.10,40
--prop:DNS_SERVERS=198,168.30,30,198,168.30,25 --prop:DOMAIN_NAME=example.com --
prop:TIMEZONE=Asia/Kolkata "C:\Program Files\CA ELM\CA Enterprise Log
Manager.ovf"
"vi://administrator:password@examplevmwarehost/ELMQAvAppDatacenter/host/10.0,10.0
"
```

Definizione delle impostazioni per la paravirtualizzazione e le risorse

Dopo aver importato il modello OVF, è necessario definire manualmente le impostazioni della paravirtualizzazione e delle risorse per migliorare le prestazioni del server CA Enterprise Log Manager di cui è stato eseguito il provisioning.

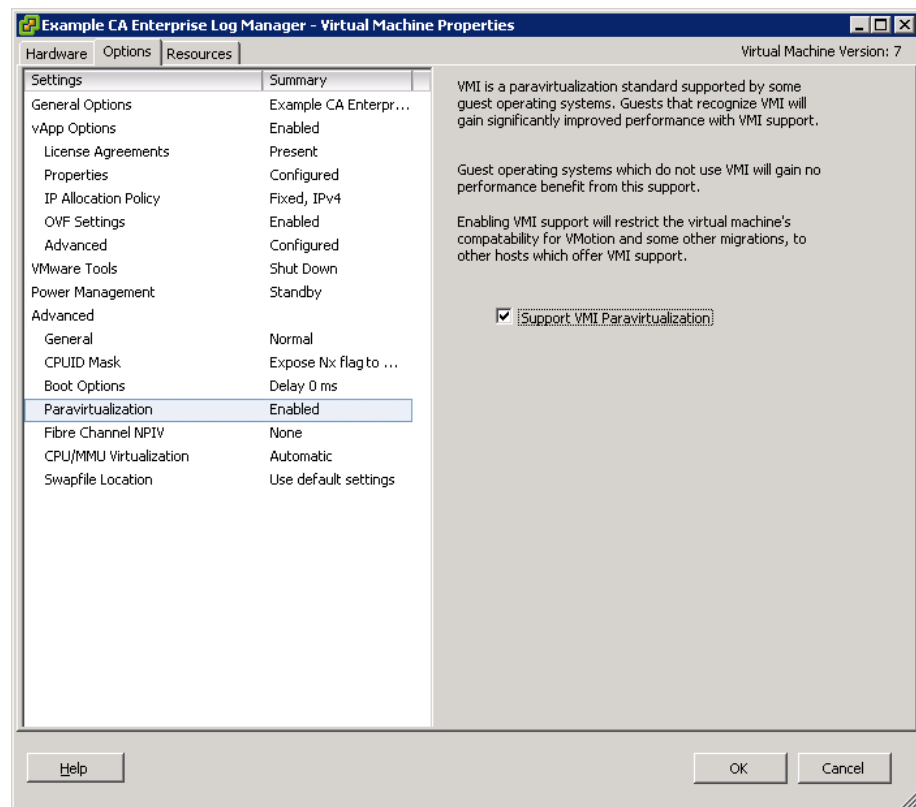
Per definire le impostazioni della paravirtualizzazione e delle risorse:

1. Fare clic con il pulsante destro del mouse sulla nuova applicazione virtuale di CA Enterprise Log Manager nel riquadro sinistro, quindi sull'opzione di modifica impostazioni.

   Viene visualizzata la finestra <*CA Enterprise Log Manager Virtual Appliance name*> - Virtual Machine Properties (Proprietà del computer virtuale <CA Enterprise Log Manager Virtual Appliance name>)

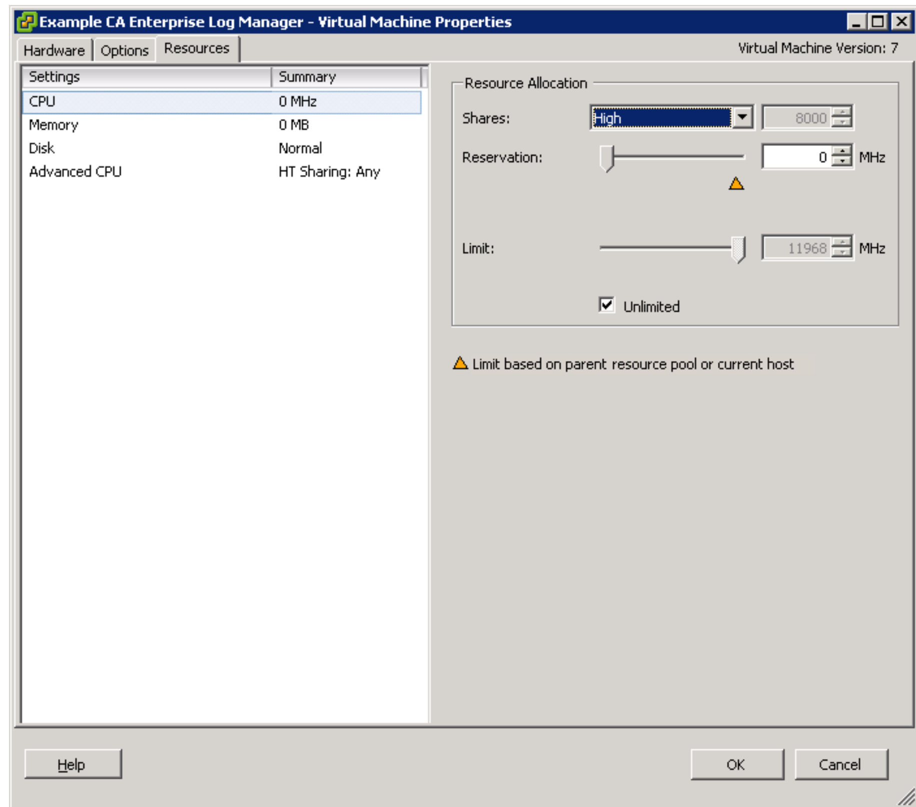
2. Fare clic sulla scheda Opzioni.

3. Selezionare l'impostazione di paravirtualizzazione nel riquadro sinistro quindi l'opzione per il supporto della paravirtualizzazione VMI nel riquadro destro.

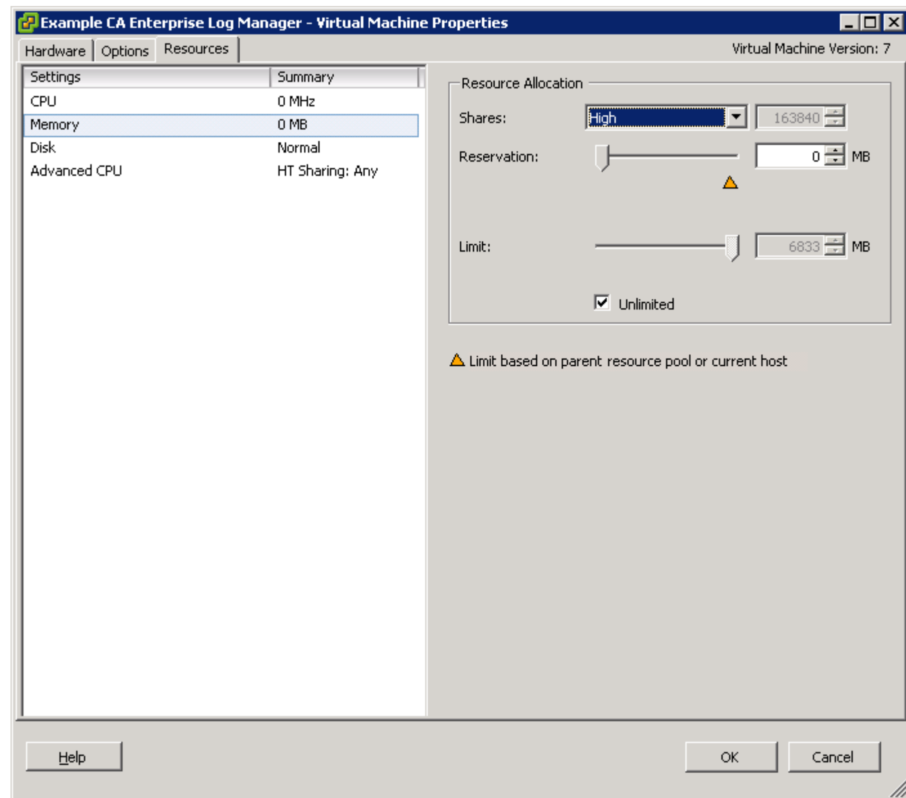


4. Fare clic sulla scheda Risorse.

5. Selezionare l'opzione CPU nella colonna Impostazioni, quindi selezionare High (Alta) dal menu a discesa Shares (Condivisioni) nella sezione Resource allocation (Allocazione risorse).



6. Selezionare l'opzione Memory (Memoria) nella colonna Impostazioni, quindi selezionare High (Alta) dal menu a discesa Shares (Condivisioni) nella sezione Resource allocation (Allocazione risorse).



7. Fare clic su OK.
8. **Nota**: per ulteriori informazioni sulla paravirtualizzazione, si rimanda al sito www.vmware.com.

Attivare il server CA Enterprise Log Manager di cui è stato eseguito il provisioning.

Il server CA Enterprise Log Manager deve essere attivato per poter dare inizio all'esecuzione.

Per attivare un server CA Enterprise Log Manager:

1. Selezionare il nuovo server CA Enterprise Log Manager nel riquadro sinistro della finestra dell'applicazione VMware.
2. Fare clic sull'opzione di avvio in Basic Tasks (Attività di base) della scheda Getting Started (Introduzione) del riquadro destro.

   Il server CA Enterprise Log Manager verrà attivato.

Nota: verificare che un server primario CA Enterprise Log Manager sia in esecuzione prima di attivare un server secondario CA Enterprise Log Manager.

Verifica dell'installazione di un server virtuale CA Enterprise Log Manager

Quando si attiva il server CA Enterprise Log Manager di cui è stato eseguito il provisioning, nella scheda della console della finestra del client VMware vSphere viene visualizzato un URL di accesso a CA Enterprise Log Manager. Utilizzare l'URL e le credenziali di accesso predefinito riportate di seguito per accedere a CA Enterprise Log Manager:

Nome utente predefinito: EiamAdmin

Password predefinita: la password immessa durante la procedura di installazione del server CA Enterprise Log Manager

Ulteriori informazioni

Aggiunta di server virtuali all'ambiente (a pagina 325)
Creazione di un ambiente completamente virtuale (a pagina 348)
Distribuzione rapida di server virtuali (a pagina 373)

Attività successive all'installazione

Dopo aver attivato un server CA Enterprise Log Manager, è possibile eseguire le operazioni riportate a continuazione:

- Modificare il tipo di tastiera
- Aggiungere un server NTP

Modifica del tipo di tastiera

Per impostazione predefinita, un server CA Enterprise Log Manager di cui è stato eseguito il provisioning utilizza la tastiera US standard. È possibile modificare il tipo di tastiera che si desidera utilizzare cambiando le impostazioni della lingua nazionali.

Per modificare il tipo di tastiera:

1. Accedere alla console CA Enterprise Log Manager come utente root.
2. Eseguire il comando:

   ```
   vi /etc/sysconfig/keyboard
   ```

   Il file di tastiera viene aperto in modalità di modifica. Vengono visualizzati i dettagli relativi al tipo di tastiera esistente.
3. Sostituire US nel valore KEYTABLE con le impostazioni nazionali della lingua che si desidera impostare.

   Ad esempio, per utilizzare la tastiera inglese (UK), immettere il valore KEYTABLE come KEYTABLE="UK".

   Nota: per ulteriori informazioni sulle impostazioni nazionali della lingua, consultare la documentazione RHEL relativa all'installazione.
4. Salvare e chiudere il file.
5. Riavviare il computer.

   Il tipo di tastiera viene modificato.

Aggiungere un server NTP

Si raccomanda vivamente di aggiungere un server NTP per procedere all'aggiornamento della data e dell'ora del server CA Enterprise Log Manager.

Per aggiungere un server NTP

1. Accedere alla console CA Enterprise Log Manager come utente root.
2. Immettere i comandi:

   ```
   crontab -e
   ```

   ```
   00 0 * * * /usr/sbin/ntpdate NTPserver_hostname
   ```

   Viene aggiunto un cron job.
3. Salvare le modifiche e uscire dalla console.

   Il server NTP viene aggiunto.

Glossario

accesso dati

Accesso dati è un tipo di autorizzazione conferita a tutti i CA Enterprise Log Manager sfruttando il Criterio predefinito di accesso ai dati., nella classe di risorsa di CALM. Ogni utente può accedere a tutti i dati, a meno che non lo si impedisca mediante dei filtri di accesso.

Accesso ODBC e JDBC

L'*accesso ODBC e JDBC* agli archivi di registro eventi di CA Enterprise Log Manager supporta l'utilizzo dei dati di evento con svariati prodotti di terze parti, inclusa la creazione di rapporti eventi personalizzati con strumenti di terze parti, la correlazione di eventi mediante motori di correlazione e la valutazione degli eventi tramite prodotti per il rilevamento di violazioni o malware. I sistemi Windows utilizzano l'accesso ODBC; i sistemi UNIX e LINUX utilizzano l'accesso JDBC.

account

Un *account* è un utente globale che è anche un utente dell'applicazione CALM. Un singolo individuo può disporre di più di un account, ognuno dei quali dotato di un diverso ruolo definito dall'utente.

adapter CA

Gli *adapter CA* sono un gruppo di listener che riceve eventi da componenti di CA Audit come i client di CA Audit e i recorder iRecorder e SAPI, oltre ad essere le origini che inviano nativamente gli eventi con iTechnology.

agente

Un *agente* è un servizio generico configurato con dei connettori, ognuno dei quali raccoglie eventi non elaborati da una singola origine evento per poi inviarli a CA Enterprise Log Manager per l'elaborazione. Ogni CALM> è dotato di un agente integrato. Inoltre, è possibile installare un agente su un punto di raccolta remoto e raccogliere gli eventi negli host in cui non si possono installare agenti. È possibile anche installare un agente su un host in cui si eseguono le origini evento, e poter quindi applicare le regole di soppressione e crittografare la trasmissione a CA Enterprise Log Manager.

agente predefinito

L'*agente predefinito* è l'agente che viene installato con il server CA Enterprise Log Manager. Può essere configurato per la raccolta diretta di eventi syslog nonché per la raccolta da diverse origini eventi non syslog come CA Access Control r12 SP1, Servizi di certificazione Microsoft Active Directory e database Oracle9i.

aggiornamenti di contenuto

Gli aggiornamenti di contenuto sono le parti non binarie degli aggiornamenti di sottoscrizione salvati nel server di gestione CA Enterprise Log Manager. Gli aggiornamenti di contenuto comprendono contenuti come i file XMP e DM, gli aggiornamenti di configurazione per i moduli di CA Enterprise Log Manager e gli aggiornamenti della chiave pubblica.

aggiornamenti di sottoscrizione

Gli aggiornamenti di sottoscrizione sono i file binari e non, distribuiti dal server di sottoscrizione diCA. I file binari sono degli aggiornamenti di modulo di prodotto solitamente installati sui CA Enterprise Log Manager. I file non binari, o aggiornamenti di contenuto, vengono memorizzati sul server di gestione.

aggregazione evento

L'aggregazione evento è il processo di consolidamento delle voci di registro simili fra loro in una singola voce contenente il numero di ricorrenze dell'evento. Le regole di riepilogo definiscono la modalità di aggregazione degli eventi.

analisi

L'analisi, detta anche analisi del messaggio, è il processo di acquisizione dei dati non elaborati di dispositivo allo scopo di trasformarli in coppie chiave-valore. L'analisi si esegue usando un file XMP. L'analisi, che precede il mapping dei dati, è un passo del procedimento di integrazione, che trasforma gli eventi non elaborati raccolti da un'origine evento in un evento perfezionato che si può visualizzare.

analisi dei file XMP

L'analisi dei file XMP è il procedimento eseguita dall'utility di Analisi del messaggio per individuare tutti gli eventi contenenti ogni stringa di corrispondenza preliminare. Si dividerà quindi ogni evento corrispondente in token in modo da poterlo analizzare utilizzando il primo filtro individuato che utilizzi la medesima stringa di corrispondenza preliminare.

analisi del mapping

L'*analisi del mapping* è un passaggio nella procedura guidata File di mapping che consente di verificare ed eseguire delle modifiche ad un file di mapping dei dati. Gli eventi campione vergono verificati tramite il file di mapping dei dati, ed i risultati si convalidano con la CEG.

analisi di messaggio

L'analisi di messaggio è il processo di applicazione delle regole all'analisi di un registro di eventi non elaborati, in modo da ottenere informazioni specifiche come il timestamp, l'indirizzo IP ed il nome utente. Le regole di analisi utilizzano la corrispondenza dei caratteri per individuare un preciso testo di evento e collegarlo ai valori selezionati.

analisi di registro

L'analisi di registro è il procedimento di estrazione dei dati da un registro, in modo che i valori analizzati possano essere utilizzati in una fase successiva della gestione di registro.

analisi di registro

L'analisi di registro è lo studio delle voci di registro utile per identificare gli eventi d'interesse. Se i registri non vengono analizzati in maniera tempestiva, il loro valore si riduce significativamente.

applicazione software

Un'*applicazione software*è un pacchetto software completamente funzionante contenente il software, il sistema operativo sottostante ed i relativi pacchetti. L'avvio del supporto di installazione consente di installare l'applicazione sull'hardware fornito dall'utente finale.

AppObject

Gli *AppObject,* o oggetti applicazione, sono risorse specifiche di prodotto memorizzate in CA EEM sotto l'istanza applicazione di un dato prodotto. Per l'istanza applicazione di CAELM, tali risorse comprendono i contenuti di rapporto e di query, le attività pianificate per i rapporti e gli avvisi, i contenuti e le configurazioni degli agenti, le configurazioni di servizi, adapter ed integrazioni, i file di mapping dei dati e di analisi del messaggio e le regole di soppressione e di riepilogo.

archiviazione automatica

L'archiviazione automatica è un procedimento configurabile che consente di automatizzare lo spostamento dei database di archivio da un server all'altro. Nella prima fase dell'archiviazione automatica, il server di raccolta invia al server di rapporto i database appena archiviati, ad intervalli specificati dall'utente. Nella seconda fase, il server di rapporto invia i database invecchiati al server di archiviazione remota per archiviarli a lungo termine, eliminando così la necessità di eseguire un backup manuale e la procedura di spostamento. Per eseguire un'archiviazione automatica, l'utente dovrà configurare un'autenticazione priva di password dal server di origine a quello di destinazione.

archiviazione di registro

L'archiviazione di registro è il processo che si verifica quando il database hot raggiunge le sue dimensioni massime, pur avendo eseguito la compressione di riga e dopo aver cambiato stato da hot a warm. Gli amministratori devono eseguire manualmente un backup dei database warm prima che sia raggiunta la soglia di eliminazione, oltre a dover eseguire l'utility LMArchive per registrare il nome dei backup. Archivia query consentirà quindi di visionare questa informazione.

archivio di catalogo

Consultare il catalogo.

archivio registro eventi

L'*archivio registro eventi* è un componente del server CA Enterprise Log Manager in cui gli eventi in arrivo si archiviano nei database. Occorre creare manualmente un backup dei database dell'archivio registro eventi, per poi spostarli su una soluzione remota di archiviazione dei registri prima dell'ora stabilita per l'eliminazione. È possibile ripristinare i database archiviati in un archivio registro eventi.

archivio registro eventi

L'archivio registro eventi è il risultato del processo di archiviazione, in cui l'utente esegue il backup di un database warm ed invia una notifica a CA Enterprise Log Manager con l'utility LMArchive. Fatto ciò, il database sottoposto a backup passerà dall'archivio registro eventi all'archivio a lungo termine.

archivio utente

Un *archivio utente* è il repository delle informazioni utente e dei criteri di password globali. Per impostazione predefinita, l'archivio utente di CA Enterprise Log Manager è il repository locale. È possibile anche configurarlo in modo da fare riferimento a CA SiteMinder o ad una directory LDAP supportata come Microsoft Active Directory, Sun One o Novell eDirectory. Indipendentemente dal modo in cui si configura l'archivio utente, il repository locale sul server di gestione contiene informazioni specifiche di applicazione sugli utenti, come ad esempio il ruolo utente e i criteri di accesso associati.

Autenticazione ssh non interattiva

L'autenticazione *non interattiva*abilita lo spostamento dei file da un server all'altro senza dover immettere una passphrase per l'autenticazione. Impostare l'autenticazione non interattiva dal server di origine al server di destinazione prima di configurare l'archiviazione automatica o di utilizzare lo script restore-ca-elm.sh.

avviso

Un *avviso* è un processo pianificato di query che è possibile utilizzare per individuare le violazioni di criterio, le tendenze di utilizzo, gli schemi di accesso e le altre informazioni che richiedono attenzione a breve termine. Per impostazione predefinita, quando la query di avviso restituisce risultati, essi verranno visualizzati nella pagina degli avvisi di CA Enterprise Log Manager e quindi aggiunti ad un feed RSS. Quando si pianifica un avviso, è possibile specificare destinazioni aggiuntive, come ad esempio la posta elettronica, un processo CA IT PAM di output di evento/avviso e i trap SNMP.

CA Enterprise Log Manager

CA Enterprise Log Manager è una soluzione utile per raccogliere i registri da origini evento di tipi diversi ed ampiamente distribuite, per verificare la conformità con le query e con i rapporti e per tener traccia dei database di registri compressi trasferiti su soluzioni esterne di archiviazione a lungo termine.

CA IT PAM

CA IT PAM corrisponde alla forma abbreviata di CA IT Process Automation Manager. Questo prodotto CA automatizza i processi definiti dall'utente. CA Enterprise Log Manager utilizza due processi: la creazione di un processo di output evento/avviso per un prodotto locale, come CA Service Desk, ed il processo di creazione dinamica di elenchi che possono essere importati come valori chiave. Per eseguire l'integrazione, è necessario disporre di CA IT PAM r2.1.

CA Spectrum

CA Spectrum è un prodotto di gestione degli errori di rete che è possibile integrare con CA Enterprise Log Manager per l'utilizzo come destinazione di avvisi inviati sottoforma di trap SNMP.

CAELM

CAELM è il nome di istanza applicazione che CA EEM utilizza per CA Enterprise Log Manager. Per accedere alle funzionalità di CA Enterprise Log Manager di CA Embedded Entitlements Manager, inserire l'URL https://<ip_address>:5250/spin/eiam/eiam.csp, selezionare CAELM come nome di applicazione, ed inserire la password dell'utente EiamAdmin.

caelmadmin

Il nome utente e la password di *caelmadmin* sono credenziali necessarie per accedere al sistema operativo dell'applicazione software. L'ID utente caelmadmin viene creato durante l'installazione di questo sistema operativo. Durante l'installazione del componente software, l'installatore deve specificare la password di EiamAdmin, ovvero dell'account di super utente di CA EEM. La stessa password verrà assegnata anche all'account caelmadmin. Si consiglia all'amministratore del server di accedere via ssh come utente caelmadmin, e di modificare la password predefinita. Anche se l'amministratore non può accedere via ssh come utente principale, potrà passare gli utenti all'account principale con il relativo comando (su root).

caelmservice

caelmservice è un account di servizio utile per eseguire iGateway ed i servizi locali di CA EEM come utente non principale. L'account caelmservice si utilizza per installare gli aggiornamenti del sistema operativo scaricati insieme agli aggiornamenti di sottoscrizione.

calendario

Un *calendario* consente di limitare il tempo di effettiva applicazione di un criterio d'accesso. Un criterio consente alle identità specificate di eseguire azioni su una risorsa in un certo periodo di tempo.

CALM

CALM è una classe di risorsa predefinita che comprende le seguenti risorse di CA Enterprise Log Manager: avviso, ArchiveQuery, calmTag, dati, EventGrouping, integrazione e rapporto. Le azioni consentite su questa classe di risorsa sono Annotazione (rapporti), Creazione (avviso, calmTag, EventGrouping, integrazione e rapporto), Dataaccess (Dati), Esecuzione (ArchiveQuery) e Pianificazione (avviso, rapporto).

calmTag

calmTag è un attributo di AppObject dotato di nome, che si utilizza creando un criterio di scoping per limitare gli utenti all'utilizzo di rapporti e query appartenenti a determinati tag. Tutti i rapporti e le query sono AppObject, e possono avere calmTag come attributo (non si deve confondere con il tag risorsa).

Campi CEG

I campi CEG sono etichette utilizzate per standardizzare la presentazione dei campi di eventi non elaborati provenienti da diverse origini evento. Durante il perfezionamento degli eventi, CA Enterprise Log Manager analizza i messaggi degli eventi non elaborati ottenendo una serie di coppie nome/valore e mappa i nomi degli eventi non elaborati ai campi CEG standard. Questo perfezionamento crea delle coppie nome/valore che consistono in campi e valori CEG provenienti dall'evento non elaborato. In altre parole, quando si perfezionano gli eventi non elaborati, le diverse etichette utilizzate in essi per lo stesso oggetto dati o elemento di rete vengono convertiti allo stesso nome di campo CEG. I campi CEG verranno mappati agli OID nella MIB utilizzata per i trap SNMP.

cartella

Una *cartella* è la posizione di un percorso di directory utilizzati dal server di gestione CA Enterprise Log Manager per memorizzare i tipi oggetto di CA Enterprise Log Manager. Nei criteri di scoping è possibile far riferimento alle cartelle per consentire o negare agli utenti di accedere ad un tipo di oggetto specifico.

catalogo

Il *catalogo* è il database in cui ogni CA Enterprise Log Manager conserva lo stato dei database archiviati, agendo anche come un indice di alto livello su tutti i database. Le informazioni di stato (warm, cold o defrosted) verranno mantenute per tutti i database presenti in questo CA Enterprise Log Manager e per qualsiasi altro database ripristinato in questo CA Enterprise Log Manager come defrosted. Le funzionalità di indicizzazione si estendono a tutti i database hot e warm nell'archivio registro eventi di questo CA Enterprise Log Manager.

categorie di evento

Le categorie di evento sono i tag utilizzati da CA Enterprise Log Manager per classificare gli eventi in base alla loro funzione, prima di inserirli nell'archivio eventi.

certificati

I *certificati* predefiniti utilizzati da CA Enterprise Log Manager sono CAELMCert.cer e CAELM_AgentCert.cer. Tutti i servizi CA Enterprise Log Manager utilizzano CAELMCert.cer per la comunicazione con il server di gestione. Tutti gli agenti utilizzano CAELM_AgentCert.cer per la comunicazione con i server di raccolta.

client di sottoscrizione

Un *client di sottoscrizione* è un server CA Enterprise Log Manager in grado di ottenere aggiornamenti di contenuto da un altro server CA Enterprise Log Manager, denominato server proxy di sottoscrizione. I client di sottoscrizione sondano regolarmente i server proxy di sottoscrizione configurati, e prelevano i nuovi aggiornamenti quando sono disponibili. Dopo aver prelevato gli aggiornamenti, il client installa i componenti scaricati.

Compatibile con FIPS 140-2

Compatibile con FIPS 140-2 designa un prodotto che può utilizzare *facoltativamente* librerie di crittografia conformi a FIPS ed algoritmi per crittografare e decrittografare dati sensibili. CA Enterprise Log Manager è una prodotto di raccolta di log compatibili con FIPS; è infatti possibile scegliere l'esecuzione in modalità FIPS o Non FIPS.

componenti di visualizzazione

I componenti di visualizzazione sono opzioni utili per visualizzare i dati di rapporto fra cui una tabella, un diagramma (a linee, a barre, a colonne e a torta), oppure un visualizzatore eventi.

configurazione globale

La *configurazione globale* è una serie di impostazioni che si applica a tutti i serverCA Enterprise Log Manager che utilizzano il medesimo server di gestione.

configurazione salvata

Una *configurazione salvata* è una configurazione archiviata con i valori degli attributi di accesso ai dati di un'integrazione, che si può utilizzare come modello per creare una nuova integrazione.

Conforme a FIPS 140-2

Conforme a FIPS 140-2 designa un prodotto che, per impostazione predefinita, utilizza *solo* algoritmi di crittografia certificati da un laboratorio accreditato di verifica dei moduli crittografici (CMT, Cryptographic Module Testing). CA Enterprise Log Manager può utilizzare moduli crittografici basati sulle librerie certificate BSAFE Crypto-C ME e Crypto-J libraries RSA in modalità FIPS. Solitamente, non si tratta tuttavia dell'impostazione predefinita.

connettore

Un *connettore* è un'integrazione per una particolare origine evento configurata su un dato agente. Un agente può caricare in memoria più connettori, di tipi simili o diversi. Il connettore consente la raccolta degli eventi non elaborati da un'origine e la trasmissione basata su regole degli eventi convertiti verso un archivio registro eventi, in cui essi saranno inseriti in un database hot. Le integrazioni out-of-the-box offrono una raccolta ottimizzata di una vasta gamma di origini evento, compresi i sistemi operativi, i database, i server Web, i firewall e molti altri tipi di applicazioni di protezione. È possibile definire un connettore per una propria origine evento da zero, oppure utilizzare un'integrazione come modello.

Contenuto dei trap SNMP

Un *trap SNMP* consiste in una serie di coppie nome/valore, in cui ogni nome è un OID (identificatore oggetto) ed ogni valore viene restituito da un avviso pianificato. I risultati di query restituiti da un avviso sono costituiti dai campi CEG e relativi valori. Il trap SNMP viene popolato sostituendo un OID per ogni campo CEG utilizzato per il nome della coppia nome/valore. La mappatura di ogni campo CEG a un OID viene memorizzata nella MIB. Il trap SNMP comprende solo le coppie nome/valore per i campi selezionati al momento di configurare l'avviso.

criterio di accesso

Un *criterio di accesso* è una regola che conferisce o nega ad un'identità (utente o gruppo utente) i diritti di accesso ad una risorsa applicazione. CA Enterprise Log Manager stabilisce se i criteri siano applicabili ad un utente specifico facendo corrispondere identità, risorse e classi di risorse, e valutando i filtri.

Criterio di accesso all'applicazione CALM

Il *Criterio di accesso all'applicazione CALM* è un tipo di elenco di controllo di accesso di un criterio di scoping che definisce chi può accedere a CA Enterprise Log Manager. Per impostazione predefinita, l'amministratore [di gruppo], l'analista [di gruppo] ed il revisore [di gruppo] potranno eseguire l'accesso.

criterio di delega

Un *criterio di delega* è un criterio di accesso che consente ad un utente di delegare la propria autorità ad un altro utente o ad un gruppo applicazione, globale o dinamico. È necessario eliminare esplicitamente i criteri di delega creati dall'utente eliminato o disattivato.

criterio di obbligo

Un *criterio di obbligo* è un criterio creato automaticamente insieme ad un filtro di accesso. Non si dovrebbe provare a creare, a modificare o ad eliminare direttamente un criterio di obbligo. Si consiglia invece di creare, di modificare o di eliminare il filtro d'accesso.

criterio di scoping

Un *criterio di scoping* è un tipo di criterio di accesso che conferisce o nega l'accesso alle risorse memorizzate nel server di gestione, come ad esempio AppObjects, utenti, gruppi, cartelle e criteri. Un criterio di scoping stabilisce quali identità possano accedere alle risorse specificate.

database archiviati

I *database archiviati* su un dato server CA Enterprise Log Manager comprendono tutti i database warm disponibili per le query per cui è necessario eseguire un backup manuale prima della scadenza, tutti i database cold registrati come sottoposti a backup e tutti quelli registrati come ripristinati dal backup.

defrosting

Il defrosting è il procedimento di modifica dello stato di un database da cold a defrosted. Questo processo viene eseguito da CA Enterprise Log Manager quando viene ricevuta una notifica dll'utility LMArchive relativa all'avvenuto ripristino di un database cold noto (se non si ripristina il database cold nel suo CA Enterprise Log Manager originale, non si dovrà utilizzare LMArchive ed eseguire il defrosting; con la ricatalogazione si aggiungerà il database ripristinato come database warm).

Destinazioni di trap SNMP

Quando si pianifica un avviso è possibile aggiungere una o più *destinazioni di trap SNMP*. Ogni destinazione di trap SNMP viene configurata con un indirizzo IP ed una porta. La destinazione è di solito un NOC o un server di gestione, come CA Spectrum o CA NSM. Quando le query per un processo di avviso pianificato restituiscono risultati verrà inviato un trap SNMP alle destinazioni configurate.

elementi di integrazione

Gli elementi di integrazione comprendono un sensore, un assistente di configurazione, un file di accesso dati ed uno o più file di analisi del messaggio (XMP) e di mapping dei dati.

elenco controllo di accesso identità

Un *elenco controllo di accesso identità* consente di specificare le diverse azioni che ogni identità selezionata può eseguire sulle risorse selezionate. Ad esempio, con un elenco di controllo accesso identità si può fare in modo che un'identità possa creare rapporti ed un'altra possa pianificarli ed annotarli. Un elenco controllo di accesso identità differisce da un elenco di controllo di accesso nel fatto che esso è incentrato sull'identità piuttosto che sulla risorsa.

event_action

event_action è il campo specifico di evento di quarto livello nella normalizzazione degli eventi utilizzata dalla CEG. Esso descrive azioni comuni. Avvio processo, Arresto processo ed Errore applicazione sono alcuni esempi di tipi di azioni evento.

event_category

event_category è il campo specifico di evento di secondo livello nella normalizzazione degli eventi utilizzata dalla CEG. Esso consente un'ulteriore classificazione degli eventi con uno specifico ideal_model. Alcuni tipi di categoria evento: Sicurezza operativa, Gestione identità, Gestione configurazione, Accesso alla risorsa e Accesso al sistema.

event_class

event_class è il campo specifico di evento di terzo livello nella normalizzazione degli eventi utilizzata dalla CEG. Esso consente un'ulteriore classificazione degli eventi in una specifica event_category.

eventi

Gli eventi in CA Enterprise Log Manager sono i record di registro generati da ogni origine evento specificata.

evento di automonitoraggio

Un *evento di automonitoraggio* è un evento registrato da CA Enterprise Log Manager. Le azioni eseguite dagli utenti entrati nel sistema, e le funzioni eseguite da diversi moduli, come i servizi e i listener, genereranno automaticamente questo tipo di eventi. È possibile visualizzare il rapporto di Dettagli eventi di automonitoraggio operazioni SIM selezionando un server di rapporto ed aprendo la scheda Eventi di automonitoraggio.

evento di osservazione

Un *evento di osservazione* è un evento che coinvolge un'origine, una destinazione ed un agente, in cui un agente di raccolta evento osserva e registra l'evento.

evento locale

Un *evento locale* è un evento che coinvolge una singola entità, in cui il medesimo host costituisce l'origine e la destinazione dell'evento. Un evento locale è il primo dei quattro tipi di evento utilizzati nella Grammatica evento comune.

evento nativo

Un *evento nativo* è lo stato o l'azione che attiva un evento non elaborato. È possibile ricevere ed analizzare o mappare gli eventi nativi come appropriato, per poi trasmetterli sotto forma di eventi perfezionati o non elaborati. Una mancata autenticazione è un evento nativo.

evento non elaborato

Un *evento non elaborato* è un'informazione attivata da un evento nativo inviata da un agente di monitoraggio al Log Manager collector. L'evento non elaborato viene spesso formattato come stringa syslog o come coppia nome-valore. In CA Enterprise Log Manager è possibile rivedere un evento nella sua forma non elaborata.

evento perfezionato

Un *evento perfezionato* è un'informazione evento mappata o analizzata che deriva da eventi non elaborati o riepilogati. CA Enterprise Log Manager esegue il mapping e l'analisi in modo che sia possibile ricercare le informazioni archiviate.

evento registrato

Si definiscono *evento registrato* le informazioni di evento non elaborate o perfezionate già inserite in un database. Gli eventi non elaborati vengono sempre registrati, a meno che non li si elimini o li si riepiloghi come avviene per gli eventi perfezionati. Si tratta di informazioni memorizzate e ricercabili.

evento remoto

Un *evento remoto* è un evento che coinvolge due diversi computer host, ovvero l'origine e la destinazione. Un evento remoto è il secondo dei quattro tipi di evento utilizzati nella Grammatica evento comune.

evento RSS

Un *evento RSS* è un evento generato da CA Enterprise Log Manager per convogliare un avviso verso prodotti ed utenti di terze parti. L'evento è un riepilogo del risultato di ogni avviso, ed un collegamento al file di risultato. È possibile configurare la durata di un dato elemento del feed RSS.

explorer agente

Explorer agente è l'archivio delle impostazioni di configurazione degli agenti (gli agenti si possono installare su un punto di raccolta o sugli endpoint in cui esistono delle origini evento).

federazione a coppie

Una *federazione a coppie* di server CA Enterprise Log Manager è una topologia che definisce una relazione paritaria fra server. Nella sua forma più semplice, il server 2 è figlio del server 1, ed il server 1 è figlio del server 2. Fra queste coppie di server vige una relazione a doppio senso. Si può definire una federazione a coppie per fare in modo che molti server siano peer l'uno dell'altro. Una query federata restituisce risultati dal server selezionato e da tutti i suoi peer.

federazione gerarchica

Una *federazione gerarchica* di server CA Enterprise Log Manager è una topologia che definisce una relazione gerarchica fra server. Nella sua forma più semplice, il server 2 è figlio del server 1, ma il server 1 non è figlio del server 2. Cioè, la relazione è a senso unico. Una federazione gerarchica può sfruttare più livelli di relazioni padre-figlio, mentre un singolo server padre può avere diversi server figlio. Una query federata produrrà risultati dai server selezionati e dai relativi figli.

file di analisi del messaggio (XMP)

Un *file di analisi del messaggio (XMP)* è un file XML, associato ad un tipo specifico di origine evento, che applica le regole di analisi. Le regole di analisi suddividono i dati rilevanti in un evento non elaborato in coppie nome-valore, che si potranno inviare al file di mapping dei dati per eseguire ulteriori elaborazioni. Questo tipo di file si utilizza in tutte le integrazioni e nei connettori, che si basano su di esse. Nel caso degli adapter CA, i file XMP si possono applicare anche al server CA Enterprise Log Manager.

file di mapping dei dati (DM)

I file di mapping dei dati (DM) sono file XML che utilizzano la Grammatica evento comune (CEG) di CA per trasformare gli eventi da un formato di origine ad uno conforme alla CEG, che sia possibile memorizzare nell'Archivio registro eventi a scopo di analisi e di creazione di rapporti. Ogni nome di registro deve disporre di un file DM prima di poter memorizzare i dati evento. Gli utenti possono modificare la copia di un file DM ed applicarla ad un determinato connettore.

filtraggio degli eventi

Il filtraggio degli eventi è il processo di rimozione degli eventi basato sui filtri di CEG.

filtro

Un *filtro* consente di porre dei limiti ad una query di archivio registro eventi.

filtro di accesso

Un *filtro di accesso* è un filtro che l'amministratore può impostare per controllare quali dati evento possano essere visualizzati dagli utenti e dai gruppi non amministrativi. Ad esempio, un filtro di accesso può ridurre i dati che alcune identità specifiche possono visualizzare in un rapporto. I filtri di accesso vengono convertiti automaticamente in criteri di obbligo.

filtro globale

Un *filtro globale* è un gruppo di criteri che possono essere specificati in modo da limitare ciò che viene mostrato in tutti i rapporti. Ad esempio, un filtro globale degli ultimi 7 giorni riporterà gli eventi generati negli ultimi sette giorni.

filtro locale

Un *filtro locale* è un gruppo di criteri che, visualizzando un rapporto, è possibile definire per limitare i dati mostrati dal rapporto corrente.

FIPS 140-2

FIPS 140-2 è lo standard federale per l'elaborazione di informazioni (FIPS, Federal Information Processing Standard). Tale standard specifica i requisiti per la sicurezza dei moduli crittografici utilizzati in un sistema di sicurezza per la protezione di informazioni sensibili ma non classificate. Lo standard fornisce quattro livelli quantitativi di miglioramento della protezione di una vasta gamma di applicazioni ed ambienti potenziali.

gestione agente

Gestione agente è il processo software che controlla tutti gli agenti associati ai CA Enterprise Log Manager federati. Può autenticare gli agenti con cui comunica.

gestione dei registri di protezione informatica

La definizione del NIST di *Gestione dei registri di protezione informatica* è la seguente: processo per generare, trasmettere, memorizzare, analizzare ed eliminare i dati di registro di protezione del computer.

gestione delle adesioni

La *gestione delle adesioni* consente di controllare ciò che gli utenti possono fare dopo l'autenticazione e l'ingresso nell'interfaccia di CA Enterprise Log Manager. È possibile ottenere tutto ciò con i criteri di accesso ed i ruoli assegnati agli utenti. I ruoli, o gruppi utente dell'applicazione, e i criteri di accesso possono essere di tipo predefinito o definito dall'utente. È l'archivio utente interno di CA Enterprise Log Manager ad occuparsi della gestione delle adesioni.

gruppo applicazione

Un *gruppo applicazione* è un gruppo specifico di prodotto che può essere assegnato ad un utente globale. I gruppi applicazione predefiniti perCA Enterprise Log Manager, o ruoli, sono amministratore, analista e revisore. Questi gruppi applicazione sono disponibili solo per gli utenti di CA Enterprise Log Manager, e non si possono assegnare agli utenti di altri prodotti registrati nel medesimo server di CA EEM. I gruppi di applicazione definiti dall'utente vanno aggiunti nel criterio di Accesso all'applicazione CALM predefinito, in modo che i suoi utenti possano accedere a CA Enterprise Log Manager.

gruppo di agenti

Un *Gruppo di agenti* è un tag che può essere applicato dagli utenti agli agenti selezionati, e che consente di applicare una configurazione agente a più agenti contemporaneamente, per poi recuperare i rapporti in base ai gruppi. Un dato agente può appartenere ad un solo gruppo alla volta. I gruppi di agenti si basano su criteri definiti dall'utente, come la regione geografica o l'importanza.

gruppo globale

Un *gruppo globale* è un gruppo condiviso fra istanze applicazioni registrate nel medesimo server di gestione di CA Enterprise Log Manager. È possibile assegnare qualsiasi utente ad uno o più gruppi globali. È anche possibile definire dei criteri di accesso con i gruppi globali come Identità a cui si consente o si impedisce di eseguire determinate azioni sulle risorse selezionate.

gruppo utenti

Un *gruppo utenti* può essere un gruppo applicazione, globale o dinamico. I gruppi applicazione predefiniti di CA Enterprise Log Manager sono amministratore, analista e revisore. Gli utenti CA Enterprise Log Manager possono appartenere ai gruppi globali sfruttando le appartenenze, indipendentemente da CA Enterprise Log Manager. L'utente può definire i gruppi dinamici e crearli attraverso un criterio di gruppo dinamico.

gruppo utenti dinamico

Un *gruppo utenti dinamico* è composto da utenti globali che condividono uno o più attributi comuni. Un gruppo utente dinamico viene creato tramite uno speciale criterio in cui il nome della risorsa è il nome del gruppo utente dinamico e l'appartenenza è basata su un set di filtri configurati in base agli attributi di utente e gruppo.

ideal_model

ideal_model è la tecnologia che esprime l'evento. Si tratta del primo campo CEG di una gerarchia di campi utilizzati per la classificazione e la normalizzazione degli eventi. Alcuni esempi di modello ideale sono gli antivirus, i DBMS, i firewall, i sistemi operativi e i server Web. I firewall Check Point, Cisco PIX e Netscreen/Juniper possono essere normalizzati con un valore di Firewall nel campo ideal_model.

identità

Un'*identità* in CA Enterprise Log Manager è un gruppo o un utente cui è consentito di accedere all'istanza applicazione di CAELM ed alle relative risorse. Un'identità per ogni prodotto CA può essere un utente globale o un utente applicazione, oppure un gruppo globale, di applicazione o dinamico.

Il NIST

Il *National Institute of Standards and Technology (NIST)*, ovvero l'Istituto nazionale degli standard e della tecnologia, è l'agenzia tecnologica federale che, nella sua pubblicazione speciale 800-92 *Guide to Computer Security Log Management (Guida alla gestione dei registri della sicurezza informatica)*, fornisce le indicazioni utilizzate come base per CA Enterprise Log Manager.

Il ruolo di amministratore

Il *ruolo di amministratore* consente agli utenti di eseguire tutte le azioni valide su ogni risorsa diCA Enterprise Log Manager. Soltanto gli amministratori possono configurare i servizi e la raccolta dei registri, o gestire gli utenti, i criteri e i filtri di accesso.

Il ruolo di analista

Il *ruolo di analista* consente agli utenti di creare e di modificare i rapporti e le query personalizzate, di modificare e di annotare i rapporti, di creare i tag e di pianificare i rapporti e gli avvisi. Gli analisti possono anche eseguire tutte le attività dei revisori.

Il ruolo di revisore

Il *ruolo di revisore* conferisce agli utenti l'accesso ai rapporti ed ai dati in essi contenuti. I revisori possono visualizzare i rapporti, l'elenco di modelli di rapporto, quello dei processi di rapporto pianificati e quello dei rapporti generati. I revisori possono anche pianificare ed annotare i rapporti. I revisori non possono accedere ai feed RSS (Rich Site Summary) a meno di impostare la configurazione in modo da non richiedere l'autenticazione per visualizzare gli avvisi.

installatore

L'*installatore* è la persona che installa l'applicazione software e gli agenti. Durante il proesso di installazione, verranno creati i nomi utente caelmadmin ed EiamAdmin, e si assegnerà a caelmadmin la password specificata per EiamAdmin. Le credenziali di caelmadmin sono necessarie per il primo accesso al sistema operativo, mentre quelle di EiamAdmin servono ad accedere per la prima volta al software CA Enterprise Log Manager e per installare gli agenti.

integrazione

L'integrazione consente di trasformare gli eventi non classificati in eventi perfezionati, in modo da poterli visualizzare nelle query e nei rapporti. È possibile implementare l'integrazione con un gruppo di elementi che consentano ad un dato agente e ad un connettore di raccogliere eventi da uno o più tipi di origini, e di inviarli a CA Enterprise Log Manager. Il gruppo di elementi comprende il sensore di registro e i file XMP e DM progettati per la lettura da un prodotto specifico. Alcuni esempi di integrazioni predefinite comprendono quelle che consentono di elaborare gli eventi syslog e WMI. È possibile creare integrazioni personalizzate per abilitare l'elaborazione degli eventi non classificati.

istanza applicazione

Una *istanza applicazione* è uno spazio comune nel repository di CA EEM in cui si memorizzano tutti i criteri, gli utenti, i gruppi, i contenuti e le configurazioni di autorizzazione. Di solito, tutti i server CA Enterprise Log Manager di un'azienda utilizzano la medesima istanza applicazione (CAELM, per impostazione predefinita). I server CA Enterprise Log Manager possono essere installati con diverse istanze applicazione, ma è possibile federare soltanto i server che condividono la medesima istanza applicazione. I server configurati per utilizzare lo stesso server CA EEM ma con diverse istanze applicazione, condividono solo l'archivio utente, i criteri di password e i gruppi globali. Diversi prodotti CA sono dotati di diverse istanze applicazione predefinite.

La grammatica evento comune (CEG, Common Event Grammar)

La Grammatica evento comune è lo schema che fornisce un formato standard in cui CA Enterprise Log Manager converte gli eventi utilizzando file di analisi e di mapping, prima di memorizzarli nell'Archivio registro eventi. La CEG utilizza campi comuni e normalizzati per definire gli eventi di protezione provenienti da diversi prodotti e piattaforme. Gli eventi impossibili da analizzare o da mappare vengono archiviati come eventi non elaborati.

libreria di analisi messaggi

La *libreria di analisi messaggi* è una libreria che riceve gli eventi dalle code dei listener e che utilizza espressioni regolari per dividere le stringhe in token, ottenendo così coppie di nomi e valori.

libreria di perfezionamento eventi

La *libreria di perfezionamento eventi* è l'archivio delle integrazioni e dei file di mapping e di analisi predefiniti o definiti dall'utente, oltre delle regole di soppressione e di riepilogo.

libreria di rapporto

La *libreria di rapporto* memorizza tutti i rapporti, i tag di rapporto, i rapporti generati e i processi di rapporto pianificati, sia predefiniti che definiti dall'utente.

libreria query

La *libreria query* memorizza tutte le query, i tag query e i filtri prompt, sia predefiniti che definiti dall'utente.

mapping dei dati

Il mapping dei dati è il processo di mapping delle coppie chiave-valore in CEG. Il mapping dei dati si esegue usando un file di mapping dei dati.

mapping di funzione

I mapping di funzione sono una parte facoltativa di un file di mapping dei dati per un'integrazione di prodotto. Il mapping di funzione si utilizza per popolare un campo CEG quando non è possibile prelevare direttamente il valore richiesto dall'evento di origine. Tutti i mapping di funzione consistono in un nome di campo CEG, in un valore di campo predefinito o di classe e nella funzione per ottenere o per calcolare il valore.

MIB

Ogni prodotto che deve ricevere avvisi da CA Enterprise Log Manager in formato di trap SNMP deve importare e compilare la *MIB (base di informazioni di gestione)* di CA Enterprise Log Manager, ovvero CA-ELM.MIB. La MIB visualizza l'origine di ogni identificatore numerico di oggetto (OID) utilizzato in un messaggio di trap SNMP con una descrizione di tale oggetto dati o elemento di rete. Nella MIB dei trap SNMP inviati da CA Enterprise Log Manager, la descrizione testuale di ogni oggetto dati si riferisce al campo CEG associato. La MIB garantisce che tutte le coppie nome/valore inviate in un trap SNMP siano interpretate in maniera corretta alla destinazione.

MIB personalizzata

Una *MIB personalizzata* è una MIB creata per un avviso inviato ad una destinazione di TRAP SNMP, come ad esempio CA NSM. L'ID di trap personalizzato specificato nell'avviso presuppone l'esistenza di una MIB personalizzata associata che definisce i campi CEG selezionati inviati come trap.

Modalità FIPS

La *modalità FIPS* è un'impostazione che richiede al server e agli agenti CA Enterprise Log Managerdi utilizzare moduli crittografici certificati FIPS di certificazione FIPS moduli di crittografia di RSA per la crittografia. L'impostazione alternativa è in modalità Non FIPS.

Modalità Non FIPS

La *modalità Non FIPS* è l'impostazione predefinita che consente ai server e agli agenti CA Enterprise Log Manager di utilizzare una combinazione di tecniche di crittografia, alcune delle quali non sono compatibili con FIPS. L'impostazione alternativa è in modalità FIPS.

modulo (da scaricare)

Un *modulo* è un raggruppamento logico di aggiornamenti componente che è possibile scaricare mediante una sottoscrizione. Un modulo può contenere aggiornamenti di file binari, di contenuto o di entrambi i tipi. Ad esempio, tutti rapporti costituiscono un modulo, mentre tutti gli aggiornamenti binari dello sponsor ne costituiscono un altro. È CA a definire ciò che costituisce ogni modulo.

modulo di sottoscrizione

Un *modulo di sottoscrizione* è un servizio che consente di scaricare automaticamente dal server di sottoscrizione CA gli aggiornamenti di sottoscrizione e di distribuirli a tutti i server e agli agenti CA Enterprise Log Manager. Le impostazioni globali si applicano ai server locali di CA Enterprise Log Manager. Le impostazioni locali indicano se un server sia un proxy non in linea, in linea, oppure un client di sottoscrizione.

nome utente EiamAdmin

EiamAdmin è il nome predefinito del super utente assegnato all'installatore dei server di CA Enterprise Log Manager. Nell'installare il primo software di CA Enterprise Log Manager, l'installatore crea una password per questo account di super utente, a meno che non esista già un server remoto di CA EEM. In questo caso, l'installatore deve inserire la password esistente. Dopo aver installato l'applicazione software, l'installatore dovrà aprire un browser da una workstation, inserire l'URL di CA Enterprise Log Manager ed accedere come EiamAdmin utilizzando la password associata. Questo primo utente imposta l'archivio utente, crea i criteri di password ed il primo account utente con ruolo di amministratore. Facoltativamente, l'utente EiamAdmin può eseguire qualsiasi operazione controllata da CA EEM.

OID

Un *OID (identificatore oggetto)* è un identificatore numerico univoco di un oggetto dati accoppiato ad un valore in un messaggio di trap SNMP. Ogni OID utilizzato in un trap SNMP inviato da CA Enterprise Log Manager viene mappato su un campo CEG testuale nella MIB. Ogni OID mappato a un campo CEG ha questa sintassi: 1.3.6.1.4.1.791.9845.x.x.x, dove 791 è il numero aziendale di CA e 9845 è l'identificatore del prodotto CA Enterprise Log Manager.

origine evento

Un'*origine evento* è l'host da cui un connettore raccoglie eventi non elaborati. Un'origine evento può contenere più archivi di registro, a ognuno dei quali un connettore separato ha avuto accesso. Distribuire un nuovo connettore comporta di solito la configurazione dell'origine evento in modo che l'agente possa accedervi e leggere eventi non elaborati da uno solo dei relativi archivi di registro. Gli eventi non elaborati del sistema operativo, di diversi database e di varie applicazioni di protezione vengono memorizzati separatamente nell'origine evento.

perfezionamento eventi

Il perfezionamento eventi è il processo in cui una stringa di un evento non elaborato viene analizzata nei campi evento che la costituiscono, per poi mapparla nei campi CEG. Gli utenti possono eseguire delle query per visualizzare i dati risultanti dell'evento perfezionato. Il perfezionamento eventi segue la raccolta e precede l'archiviazione degli eventi.

plugin evento iTech

Il *plugin evento iTech* è un adapter CA che un amministratore può configurare con i file di mapping selezionati. Riceve eventi dagli iRecorder remoti, da CA EEM, dallo stesso iTechnology, o da qualsiasi prodotto che consenta di inviare eventi usando iTechnology.

pozFolder

pozFolder è un attributo di AppObject, il cui valore è il percorso padre di AppObject. L'attributo ed il valore di pozFolder vengono utilizzati nei filtri dei criteri di accesso che limitano l'accesso a risorse come rapporti, query e configurazioni.

Procedura guidata file di analisi

La *Procedura guidata file di analisi* è una funzione di CA Enterprise Log Manager che gli amministratori possono utilizzare per creare, modificare ed analizzare i file XMP (eXtensible Message Parsing) memorizzati nel server di gestione di CA Enterprise Log Manager. Per personalizzare l'analisi dei dati evento in arrivo è necessario modificare le stringhe ed i filtri di corrispondenza preliminare. I file nuovi e quelli modificati vengono visualizzati in Explorer raccolta registri, in Libreria di perfezionamento eventi, in File di analisi e nella cartella Utente.

processo di output evento/avviso

Il *processo di output evento/avviso* è il processo CA IT PAM che richiama un prodotto di terze parti per rispondere ai dati di avviso configurati in CA Enterprise Log Manager. Quando si pianifica un processo di avviso, è possibile selezionare come destinazione il Processo CA IT PAM. Quando un avviso esegue il processo CA IT PAM, CA Enterprise Log Manager invia i dati di avviso a CA IT PAM, il quale li inoltra al prodotto di terze parti con i parametri di elaborazione CA IT PAM, nell'ambito del processo di output evento/avviso.

processo valori dinamici

Un *processo di valori dinamici* è un processo CA IT PAM che è possibile selezionare per compilare o aggiornare l'elenco dei valori di una chiave selezionata utilizzata in rapporti o avvisi. Durante la configurazione di IT PAM, l'utente fornisce il percorso al Processo valori dinamici nell'Elenco del servizio dei server di rapporto, nella scheda Amministrazione. Dopodiché, l'utente fa clic sull'elenco Importa valori dinamici nella sezione Valori associata ai Valori principali sulla stessa pagina dell'interfaccia utente. Richiamare il processo valori dinamici è uno dei tre metodi che consentono di aggiungere valori alle chiavi personali.

profilo

Un *profilo* è un gruppo di tag e di filtri dati opzionale e configurabile, che può essere specifico del prodotto, della tecnologia o limitato ad una data categoria. Un filtro tag di un prodotto, ad esempio, limita i tag elencati a quelli del prodotto specificato. I filtri dati di un prodotto visualizzano, nei rapporti generati dall'utente, negli avvisi pianificati e nei risultati delle query, solo i dati per il prodotto specificato. Dopo aver creato il profilo necessario, lo si può impostare in modo che sia effettivo subito dopo aver eseguito l'accesso. Se si creano più profili, durante una sessione si potranno applicare diversi profili alle proprie attività, a patto di farlo uno per volta. I filtri predefiniti vengono distruibiti insieme agli aggiornamenti di sottoscrizione.

prompt

Un *prompt* è un tipo speciale di query che visualizza risultati in base al valore inserito ed ai campi di CEG selezionati dall'utente. Vengono restituite righe solo per gli eventi in cui il valore inserito dall'utente viene visualizzato in uno o più campi di CEG selezionati.

proxy di sottoscrizione (in linea)

Un *proxy di sottoscrizione in linea* è un CA Enterprise Log Manager con accesso ad Internet in grado di ottenere aggiornamenti di sottoscrizione da un server di sottoscrizione diCA con una pianificazione ricorrente. È possibile includere un dato proxy di sottoscrizione in linea nell'elenco dei proxy di uno o più client, che possono contattare in maniera circolare i proxy elencati per richiedere gli aggiornamenti binari. Un dato proxy online, se configurato in questo modo, invierà i nuovi contenuti e gli aggiornamenti di configurazione al server di gestione, a meno che un altro proxy non abbia già eseguito tale operazione. La directory di aggiornamento di sottoscrizione di un proxy in linea selezionato verrà utilizzata come origine per la copia degli aggiornamenti nei proxy di sottoscrizione non in linea.

proxy di sottoscrizione (non in linea)

Un *proxy di sottoscrizione non in linea* è un server CA Enterprise Log Manager che può ottenere aggiornamenti di sottoscrizione eseguendo una copia manuale di directory (usando scp) da un proxy di sottoscrizione in linea. È possibile configurare i proxy di sottoscrizione non in linea in modo da scaricare i file binari di aggiornamento sui client che li richiedono, ed inviare l'ultima versione degli aggiornamenti di contenuto al server di gestione, nel caso in cui esso non li abbia già ricevuti. I proxy di sottoscrizione non in linea non richiedono un accesso ad Internet.

proxy di sottoscrizione (per gli aggiornamenti di contenuto)

I *proxy di sottoscrizione per gli aggiornamenti di contenuto* sono i proxy di sottoscrizione scelti per aggiornare il server di gestione CA Enterprise Log Manager con gli aggiornamenti di contenuto scaricati dal server di sottoscrizione CA. È consigliabile configurare più proxy per la ridondanza.

proxy di sottoscrizione (per il client)

Il *proxy di sottoscrizione per il client* integra l'elenco di proxy di sottoscrizione che il client può contattare in maniera circolare per ottenere il software CA Enterprise Log Manager e gli aggiornamenti del sistema operativo. Se un proxy è occupato, verrà contattato il successivo nella lista. Nel caso fossero tutti occupati ed il client sia in linea, si utilizzerà il proxy di sottoscrizione predefinito.

proxy di sottoscrizione (predefinito)

Il *proxy di sottoscrizione predefinito* è di solito il server CA Enterprise Log Manager installato per primo, oppure anche il CA Enterprise Log Manager principale. Il proxy di sottoscrizione predefinito è anche un proxy di sottoscrizione in linea, e deve pertanto disporre di un accesso ad Internet. Se non si definiscono altri proxy di sottoscrizione, tale server otterrà gli aggiornamenti di sottoscrizione dal server di sottoscrizione CA e scaricherà gli aggiornamenti binari su tutti i client, per poi inviare ad CA EEM gli aggiornamenti di contenuto. Se si definiscono altri proxy, tale server riceverà ugualmente gli aggiornamenti di sottoscrizione. I client per gli aggiornamenti, però, lo contatteranno solo quando non verrà configurato nessun elenco di proxy di sottoscrizione, o quando tale elenco sarà esaurito.

punto di raccolta

Un *punto di raccolta* è un server su cui si installa un agente, dotato di prossimità di rete con tutti i server che dispongono di origini evento associate ai connettori del proprio agente.

query

Una *query* è un gruppo di criteri utilizzato per cercare negli archivi registro evento del server CA Enterprise Log Manager attivo e, se specificati, nei suoi server federati. Una query agisce sui database hot, warm o defrosted specificati nella sua clausola Dove. Per esempio, se la clausola Dove limita la query agli eventi con source_username="myname" in un determinato intervallo di tempo, e se solo 10 dei 1000 database contengono record corrispondenti a questo criterio in base alle informazioni nel database di catalogo, la query agirà solo su questi dieci database. Una query può produrre un massimo di 5000 righe di dati. Qualsiasi utente con un ruolo predefinito può eseguire una query. Solo gli analisti e gli amministratori possono pianificare una query per distribuire un avviso, per creare un rapporto selezionando le query da inserire o per creare una query personalizzata utilizzando la procedura guidata Progettazione query. Consultare anche Archivia query.

query azione

Una *query azione* è una query che supporta un avviso. Si esegue con pianificazione ricorrente allo scopo di verificare le condizioni delineate dall'avviso cui essa è allegata.

query di archiviazione

Una *query di archiviazione* è una query del catalogo utile per identificare i database cold che necessitino di un ripristino e di un defrost per poter eseguire una query. Una query di archiviazione differisce da una normale. Essa agisce infatti sui database cold, mentre una query normale agisce sui database hot, warm e defrosted. Gli amministratori possono eseguire una query di archiviazione dalla scheda Amministrazione, sottoscheda Raccolta registri, opzione Archivia query di catalogo.

raccolta eventi

La raccolta eventi è il processo di lettura delle stringhe degli eventi non elaborati da un'origine evento, per poi inviarli al CA Enterprise Log Manager configurato. Il perfezionamento eventi avverrà dopo la raccolta di eventi.

raccolta registri diretta

La raccolta registri diretta è la tecnica di raccolta dei registri in cui non esiste alcun agente intermedio fra l'origine evento ed il software CA Enterprise Log Manager.

Rapporti relativi ad EPHI

I *rapporti relativi a EPHI* sono rapporti incentrati sulla protezione HIPAA, in cui EPHI significa Informazioni sanitarie elettroniche protette (Electronic Protected Health Information). Tali rapporti consentono di dimostrare la protezione della creazione, della manutenzione e della trasmissione elettronica di tutte le informazioni sanitarie singolarmente identificabili e correlate ai pazienti.

rapporto

Un *rapporto* è una visualizzazione grafica o tabulare dei dati del registro eventi generata eseguendo query predefinite o personalizzate con filtri. I dati provengono da database hot, warm o defrosted dell'archivio registro eventi del server selezionato e, se richiesto, dei server federati.

record di controllo

I record di controllo contengono eventi di protezione come i tentativi di autenticazione, gli accessi ai file e le modifiche ai criteri di protezione, agli account utente o ai privilegi. Gli amministratori possono specificare quale tipo di evento controllare e quale inserire nei registri.

record di registro

Un *record di registro* è un singolo record di controllo.

registro

Un *registro* è un record di controllo, o messaggio registrato, di un evento o di una raccolta di eventi. Un registro può essere di controllo, di transazione, di intrusione, di connessione, di prestazioni di sistema, di attività utente o di avviso.

regole di riepilogo

Le regole di riepilogo sono regole che uniscono alcuni eventi nativi di tipo comune ottenendo così un unico evento perfezionato. Ad esempio, è possibile configurare una regola di riepilogo per sostituire fino a 1000 eventi duplicati, con gli stessi indirizzi IP e porte di origine e di destinazione, con un singolo evento di riepilogo. Regole di questo tipo semplificano l'analisi degli eventi e riducono il traffico di registro.

regole di soppressione

Le regole di soppressione sono delle regole da configurare per impedire ad alcuni eventi perfezionati di apparire nei propri rapporti. È possibile creare regole di soppressione permanenti per eliminare gli eventi di routine che non riguardano la protezione, oltre a creare regole temporanee per eliminare la registrazione di eventi pianificati come la creazione di molti nuovi utenti.

regole inoltro eventi

Le regole *inoltro eventi* indicano che gli eventi selezionati sono da inoltrare a prodotti di terze parti, ad esempio i prodotti che stabiliscono la correlazione tra eventi, una volta salvati nell'archivio di registro eventi.

ricatalogazione

Una *ricatalogazione* è la ricostruzione forzata del catalogo. Si deve eseguire una ricatalogazione solo quando si ripristinano dei dati di un archivio registro eventi su un server diverso da quello in cui è stato generato. Ad esempio, se si sceglie un CA Enterprise Log Manager che agisca come punto di ripristino per le analisi sui dati cold, si potrebbe dover forzare una ricatalogazione del database dopo averlo ripristinato nel punto di ripristino scelto. Se necessario, la ricatalogazione si avvierà automaticamente al riavvio di iGateway. La ricatalogazione di un singolo file di database può impiegare anche diverse ore.

risorsa applicazione

Una *risorsa applicazione* è una delle risorse specifiche di CA Enterprise Log Manager per cui i criteri di accesso di CALM consentono o negano alle identità specificate di eseguire azioni specifiche dell'applicazione come creare, pianificare e modificare. Alcuni esempi di risorse applicazione sono il rapporto, l'avviso e l'integrazione. Consultare anche Risorsa globale.

risorsa globale

Una *risorsa globale* del prodotto CA Enterprise Log Manager è una risorsa condivisa con altre applicazioni CA. È possibile creare criteri di scoping con risorse globali. Alcuni esempi sono l'utente, il criterio ed il calendario. Consultare anche Risorsa applicazione.

ruolo utente

Un *ruolo utente* può essere un gruppo applicazione predefinito o un gruppo applicazione definito dall'utente. Sono necessari ruoli utente personalizzati quando i gruppi applicazione predefiniti (amministratore, analista e revisore) non sono sufficientemente dettagliati per riflettere le assegnazioni del lavoro. I ruoli utente personalizzati richiedono criteri di accesso personalizzati e la modifica dei criteri predefiniti per includere il nuovo ruolo.

SafeObject

SafeObject è una classe di risorsa predefinita di CA EEM. È la classe di risorsa memorizzata sotto l'ambito di Applicazione, ed a cui appartiene AppObjects. Gli utenti che definiscono criteri e filtri per consentire l'accesso ad AppObjects fanno riferimento a questa classe di risorse.

SAPI collector

SAPI collector è un adapter CA che consente di ricevere eventi dai client di CA Audit. I client di CA Audit inviano tramite l'azione Raccoglitore, che fornisce un failover integrato. Gli amministratori configurano CA Audit SAPI Collector con, ad esempio, le crittografie ed i file di mapping dei dati selezionati.

SAPI recorder

Il *SAPI recorder* era la tecnologia utilizzata per inviare informazioni a CA Audit prima di iTechnology. SAPI significa Submit API (Inviare interfaccia di programmazione di applicazione, Submit Application Programming Interface). I recorder di CA Audit per CA ACF2, CA Top Secret, RACF, Oracle, Sybase e DB2 sono esempi di SAPI recorder.

SAPI router

Il *SAPI router* è un adapter CA in grado di ricevere eventi dalle integrazioni, come Mainframe, per poi inviarle ad un router di CA Audit.

sensore di registro

Un *sensore di registro* è un componente di integrazione progettato per leggere un tipo specifico di registro, come database, syslog, file o SNMP. I sensori di registro possono essere riutilizzati. Di solito, gli utenti non creano sensori di registro personalizzati.

server avvisi

Il *server avvisi* è l'archivio degli avvisi e dei relativi processi.

server del punto di ripristino

Un *server del punto di ripristino* è un ruolo ricoperto da un server CA Enterprise Log Manager. Per analizzare gli eventi "cold", è possibile usare un'utility per spostare i database dal server di archiviazione remota a quello del punto di ripristino, per poi aggiungerli al catalogo ed eseguire delle query. Lo spostamento dei database cold in un punto di ripristino dedicato è un'alternativa al riportarli nel server di rapporto originale in modo da poter eseguire delle analisi.

server di archiviazione remota

Un *server di archiviazione remota* è un ruolo assegnato ad un server che riceva i database archiviati automaticamente da uno o più server di rapporto. Un server di archiviazione remota memorizza i database cold per il numero di anni necessari. Di solito non conviene installare CA Enterprise Log Manager, o altri prodotti, negli host remoti per la memorizzazione. Per l'archiviazione automatica, configurare l'autenticazione non interattiva.

server di federazione

I server di federazione sono server CA Enterprise Log Manager collegati l'un l'altro nella rete per distribuire la raccolta dei dati di registro, ma aggregando i dati raccolti in modo da creare un rapporto. I server di federazione possono essere collegati tramite una topologia gerarchica o a coppie. I rapporti dei dati federati comprendono quelli provenienti dal server di destinazione, oltre a quelli provenienti dai figli o dai peer di tale server, se presenti.

server di gestione

Il *server di gestione* è un ruolo assegnato al primo server CA Enterprise Log Manager installato. Questo server CA Enterprise Log Manager contiene il repository che contiene i contenuti condivisi per tutti i CA Enterprise Log Manager, come ad esempio i criteri. Tale server è di solito il proxy predefinito di sottoscrizione. Il server di gestione può ricoprire tutti i ruoli, anche se si tratta di una pratica sconsigliata per la maggior parte degli ambienti di produzione.

server di raccolta

Un *server di raccolta* è un ruolo ricoperto da un server CA Enterprise Log Manager. Il server di raccolta rifinisce i registri evento in arrivo e li inserisce nel database hot. Fatto ciò, comprime ed archivia automaticamente, o copia, tale database nel server di rapporto correlato. Il server di raccolta comprime il database hot quando esso raggiunge le dimensioni configurate, e lo archivia automaticamente seguendo la pianificazione configurata.

server di rapporto

Il *server di rapporto* è il servizio che archivia informazioni di configurazione come il server da utilizzare nell'inviare gli avvisi via posta elettronica, l'aspetto visivo dei rapporti salvati in formato PDF, la memorizzazione dei criteri per i rapporti salvati nel server di rapporto e gli avvisi inviati al feed RSS.

server di rapporto

Un *server di rapporto* è un ruolo ricoperto da un server CA Enterprise Log Manager. Un server di rapporto riceve database warm archiviati automaticamente da uno o più server di raccolta. Un server di rapporto può gestire query, rapporti, avvisi e rapporti pianificati.

server di sottoscrizione CA

Il *server di sottoscrizione CA* è l'origine degli aggiornamenti di sottoscrizione da CA.

Server ODBC

Il *server ODBC* è il servizio configurato che imposta la porta utilizzata per le comunicazioni tra il client ODBC o JDBC e il server CA Enterprise Log Manager e specifica se utilizzare la crittografia SSL.

server proxy HTTP

Un *server proxy HTTP* è un server proxy in grado di agire come firewall, impedendo al traffico Internet di entrare o uscire dall'azienda se non attraverso il proxy. Il traffico in uscita può specificare un ID e una password che consentano di bypassare il server proxy. È possibile configurare l'utilizzo di un server proxy HTTP locale nella gestione delle sottoscrizioni.

servizi

I *servizi* CA Enterprise Log Manager sono l'archivio registro eventi, il server di rapporto e la sottoscrizione. Gli amministratori possono configurare tali servizi a livello globale dove, per impostazione predefinita, tutte le impostazioni si applichino ad ogni CA Enterprise Log Manager. La maggior parte delle impostazioni globali per i servizi si possono ignorare a livello locale, ovvero per ogni CA Enterprise Log Manager specificato.

SNMP

SNMP è l'acronimo di protocollo di gestione di rete semplice (Simple Network Management Protocol), uno standard aperto per l'invio di messaggi di avviso sottoforma di trap SNMP da un sistema di agente ad uno o più sistemi di gestione.

soppressione

La soppressione è il processo di rimozione degli eventi in base ai filtri di CEG. La soppressione si esegue usando file SUP.

stati del database

Gli *stati del database* sono i seguenti: hot, per i database non compressi costituiti da nuovi eventi; warm, per un database di eventi compressi; cold, per un database sottoposto a backup; defrosted, per un database ripristinato nell'archivio registro eventi da cui è stato eseguito il backup. È possibile eseguire query sia su database hot che warm e defrosted. Una query di archiviazione visualizza informazioni sui database cold.

stato di database cold

Lo *stato di database cold* si applica ad un database warm quando un amministratore esegue LMArchive per avvertire CA Enterprise Log Manager dell'avvenuta esecuzione di un backup del database. Gli amministratori devono eseguire i backup dei database warm, ed eseguire questa utility prima della loro eliminazione. Un database warm verrà automaticamente cancellato quando la sua età supererà il valore indicato in Numero massimo di giorni di archiviazione, oppure quando si raggiungerà la soglia dello Spazio su disco di archiviazione, indipendentemente da quale dei due si verifichi prima. È possibile eseguire una query sul database di archiviazione per identificare i database con stato warm e cold.

stato di database defrosted

Uno *stato di database defrosted* è quello applicato ad un database ripristinato nella directory di archiviazione dopo che l'amministratore ha eseguito l'utility LMArchive per avvisare CA Enterprise Log Manager dell'avvenuto ripristino. I database defrosted si conservano per il numero di ore configurate in Criterio di esportazione. È possibile eseguire una query di registri evento nei database di stato hot, warm e defrosted.

stato di database hot

Uno *stato di database hot* è lo stato di un database dell'archivio registro eventi nel momento in cui si inseriscono nuovi eventi. Quando il database hot raggiunge dimensioni configurabili sul server di raccolta, lo si comprime, cataloga e trasferisce in un archivio warm sul server di rapporto. Inoltre, tutti i server memorizzano i nuovi eventi di automonitoraggio in un database hot.

stato warm del database

Lo *stato warm del database* è quello in cui un database hot di registri evento si evolve quando si superano le dimensioni (Numero massimo di righe) di quest'ultimo, oppure quando si esegue una ricatalogazione dopo il ripristino di un database cold in un nuovo archivio registro eventi. I database warm vengono compressi e conservati nell'archivio registro eventi fino a quando la loro età in giorni supera il valore configurato per Numero massimo di giorni di archiviazione. È possibile eseguire una query di registri evento nei database di stato hot, warm e defrosted.

tag

Un *tag* è un termine o una frase chiave utilizzata per identificare i rapporti o le query che appartengono allo stesso gruppo relativo ai business. I tag consentono di eseguire ricerche basate sui gruppi relativi ai business. Tag è anche il nome di risorsa utilizzato in qualsiasi criterio che consenta agli utenti di creare un tag.

token di analisi del messaggio (ELM)

Un *token di analisi del messaggio* è un modello riutilizzabile per costruire la sintassi dell'espressione regolare utilizzata da CA Enterprise Log Manager per l'analisi del messaggio. Un token possiede un nome, un tipo ed una stringa della corrispondente espressione regolare.

URL del feed RSS per gli avvisi

L'*URL del feed RSS per gli avvisi* è: https://{elmhostname}:5250/spin/calm/getActionQueryRssFeeds.csp. Da questo URL è possibile visualizzare gli avvisi sulle azioni soggetti alla configurazione di età e quantità massime.

URL del feed RSS per la sottoscrizione

L'*URL del feed RSS per la sottoscrizione* è un collegamento preconfigurato utilizzato dai server proxy di sottoscrizione in linea per recuperare gli aggiornamenti di sottoscrizione. Questo URL vale per il server di sottoscrizione CA.

URL di CA Embedded Entitlements Manager

L'*URL di CA Embedded Entitlements Manager* (CA EEM) è: https://<ip_address>:5250/spin/eiam. Per accedere, selezionare CAELM come applicazione ed inserire la password associata al nome utente EiamAdmin.

URL di CA Enterprise Log Manager

L'*URL di CA Enterprise Log Manager* è: https://<ip_address>:5250/spin/calm. Per accedere, inserire il nome utente del proprio account definito dall'amministratore e la password associata. Oppure, inserire il nome predefinito del super utente EiamAdmin e la password associata.

utente applicazione

Un *utente applicazione* è un utente globale a cui si assegnano dettagli a livello di applicazione I dettagli utente dell'applicazione CA Enterprise Log Manager comprendono il gruppo utente e qualsiasi restrizione di accesso. Se l'archivio utente è il repository locale, i dettagli utente dell'applicazione conterranno anche le credenziali di accesso e criteri di password.

Utente EEM

L'*Utente EEM*, configurato nella sezione di archiviazione automatica dell'archivio registro eventi, indica l'utente che può eseguire una query di archiviazione, ricatalogare il database di archivio ed eseguire l'utility LMArchive e lo script shell restore-ca-elm per ripristinare i database d'archiviazione in modo da poterli analizzare. Si deve assegnare a tale utente il ruolo predefinito di amministratore, oppure uno personalizzato associato ad un criterio personalizzato che consenta l'azione di modifica sulla risorsa Database.

utente globale

Un *utente globale* è l'informazione dell'account utente che esclude i dettagli specifici dell'applicazione. I dettagli dell'utente globale e le appartenenze al gruppo globale sono condivisi in tutte le applicazioni CA che si integrano con l'archivio utente predefinito. È possibile memorizzare i dettagli dell'utente globale nel repository integrato oppure in una directory esterna.

utility LMArchive

L'*utility LMArchive* si esegue dalla linea di comando, e tiene traccia del procedimento di backup e di ripristino dei database di archivio nell'archivio registro eventi di un server CA Enterprise Log Manager. Utilizzare LMArchive per eseguire una query utile per ottenere l'elenco dei database warm pronti per l'archiviazione. Dopo aver eseguito il backup del database elencato ed averlo spostato nell'archivio a lungo termine (cold), utilizzare LMArchive per creare un record su CA Enterprise Log Manager che indichi l'avvenuta esecuzione del backup di questo database. Dopo l'avvenuto ripristino di un database cold nel suo CA Enterprise Log Manager originale, utilizzare LMArchive per inviare una notifica a CA Enterprise Log Manager, che a sua volta trasformerà i file del database in stato defrosted, in modo da poter ricevere delle query.

utility LMSEOSImport

L'*utility LMSEOSImport* è un'utility da riga di comando e consente di importare SEOSDATA o eventi esistenti in CA Enterprise Log Manager, durante la migrazione da Audit Reporter, da Viewer o da Audit Collector. Solo Microsoft Windows e Sun Solaris Sparc supportano questa utility.

utility scp

L'utility *scp*, copia sicura, (un programma di copia di file remoti) è un'utility UNIX che consente di trasferire file fra i diversi computer UNIX in una rete. È possibile utilizzare questa utility subito dopo l'installazione di CA Enterprise Log Manager, per trasferire i file di aggiornamento di sottoscrizione dal proxy di sottoscrizione in linea a quello non in linea.

valori principali

I valori principali sono valori definiti dell'utente ed assegnati a un elenco anch'esso definito dall'utente (gruppo principale). Quando una query utilizza un gruppo principale, i risultati della ricerca contengono le corrispondenze a qualsiasi valore principale presente nel gruppo principale. Esistono diversi gruppi principali predefiniti utilizzati nelle query e nei rapporti predefiniti. Alcuni gruppi contengono valori principali predefiniti.

varbind

Una *varbind* è un binding di variabile SNMP. Ciascuna varbind è costituita da un OID, un tipo, ed un valore. Le varbind vengono aggiunte alle MIB personalizzate.

voce di registro

Una *voce di registro* è una voce in un registro contenente informazioni su un evento specifico verificatosi nel sistema o in una rete.

Indice

R

S

T

U